Jurnal Hubungan Internasional
Indonesia

http://jhii.fisip.unila.ac.id/ojs/index.php/jhii

CHINA'S ECONOMIC CYBER ESPIONAGE TOWARD THE UNITED STATES AS A NATIONAL SECURITY THREAT

Harryanto Aryodiguno, Ph.D[1], Ong, Yohana Novencia Havisaputra[2]
[1] Hubungan Internasional, Universitas Presiden, Indonesia,
[2] Hubungan Internasional, Universitas Presiden, Indonesia,
harry_anto@president.ac.id

Abstract

Technological developments in the realm of cyberspace have triggered the emergence of new challenges in the form of economic cyber espionage involving the theft of trade secrets and intellectual property which pose a threat to national security. This problem started to receive special attention after the report of economic cyber espionage crimes committed by China against domestic American companies in 2010. In dealing with issues that threaten the country's national security, the United States government has decided to implement a strategy, one of which prioritizes the use of diplomacy. With the cooperation conducted by the United States government, the number of economic cyber espionage cases can finally decrease, and this shows that the use of cyber diplomacy can be the best step to deal with cases of crime in cyberspace. Furthermore, the effectiveness of the strategy adopted by the United States in dealing with the threat of economic cyber espionage from China, especially in 2010 to 2015, will be analyzed more deeply by using the concept of cyber diplomacy through secondary data collection methods.

Keywords: Cyber Diplomacy, Cybercrime, Economic Cyber Espionage, United States, China

Introduction

Following the advancement of technology in the contemporary era, the term 'cyberspace' has been widely known and has become part of daily life for modern society. Cyberspace managed to appear until it became the 'fifth domain' of human activity beside land, sea, air, and outer space as this environment slowly blended into people's life within these few decades (Buchan, 2019). However, amidst the development of cyberspace, the occurrence of numerous cyber threats in the form of cybercrime has brought new challenges that not only haunted certain parties but almost all of the global community without any exception. Even the fact that in cyber crime there are no such things like the DNA sample or fingerprints to identify the perpetrator has made it easier for the criminals in cyberspace to hide and hard to be found through the use of proxy servers, virtual private networks, or peer-to-peer software (Handford, 2014). Only the time zone, location of the physical servers used in the attack, nation-specific tools and techniques, and language indicators of the perpetrators are able to be analyzed by the researchers (Ibid.). This situation

then develops and creates a more complex taxonomy where the range of cyber threats now is getting wider.

The emergence of ‘cyber espionage' or well-known as ‘cyber spying’ which managed to gain attention from global society as a concerning issue also added to the long list of threats in cyberspace. Cyber espionage often involves states as the most prolific perpetrators and can be divided into two categories depending on the kind of information that is being collected, which are political espionage and economic espionage. Different from political espionage which is used for deriving political and military information owned by other state or non-state actors with the purpose to increase national security (Buchan, 2019), economic espionage aims to boost the country's national economy by stealing and giving confidential information related with the trade secret held by foreign private corporations to the domestic companies (Fidler, 2013). A country such as the United States defines economic espionage as “foreign power-sponsored or coordinated intelligence activity directed at the U.S. government or U.S. corporations, establishments, or persons, designed to unlawfully or clandestinely influence sensitive economic policy decisions or to unlawfully obtain sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies” (FBI, 2016). In the beginning, economic espionage was actually considered to be important for national security and economic development for a long time by most countries (Fidler, 2013), until the international proliferation of the internet has changed cyber economic industrial espionage into an exceptional threat that is even possible to cause economic crippling (O'Hara, 2010).

Although in the past companies more or less tend to ignore the issue regarding the foreign governments' infiltration in their companies' electronic network that has been conducted for almost a quarter century through the exploitation of internet connectivity, since 2010 the economic cyber espionage issue has now been identified as a growing threat. The reason behind this is because economic cyber espionage that seeks to steal the secrets owned by foreign companies, sometimes also potentially involves intellectual property theft that brings comparative economic advantage for the perpetrator states or their proxies to secure trade negotiation, certain deals, or for the sake of specific enterprises (Banks, 2017). As a result, companies that become the victim of cyber espionage will suffer from financial struggles caused by the direct and indirect costs and shaking financial stability as the impact of cyber espionage. Meanwhile, if those companies are facing a financial downturn, the adverse effect on the national economy of the host country is unavoidable, and with the consideration that today’s national security is contingent based on economic security, hence, economic espionage is an imposing threat to national security and by international peace and security implication (Buchan, 2019).

The United States, a country with strong economic power, also acknowledges the problem regarding cyber espionage as a concerning issue in its country that even impacted the country's bilateral relations. This country eventually admitted that cyber economic espionage can be a threatening issue after one of its biggest technological companies, Google Inc., along with dozens of other American companies have become the victims of cyber spying. In this case, the United States put the blame on China since according to security experts, companies that become the victims are those within strategic industries in which China is still lagging (O'Hara, 2010). Therefore, in the network security field, the relations between the United States and China can be put in three stages: "Mutual benefit and win-win stage (1994-1999), The Sino-US network relationship is roughly balanced. (1999-2010), The frequent occurrence of network security issues (2010-present)" (Qian, 2019).

Nevertheless, in international law, all cyber activities related to espionage are neither lawful nor unlawful since the international legal system does not regulate espionage, or in other words, every state is free to conduct espionage and *vice versa* also accept it from the other states with the prosecution of spies under domestic law and expulsion of ambassadors as the only consequences (Brown, 2016). Together with other like-minded countries, the United States, who previously agreed that spies should be punished according to domestic law, decided to change its position and believed that not all cyber espionage is acceptable to state behaviour (Libicki, 2017). The United States argues that traditional espionage aims to acquire the protected information of foreign governments, while on the other hand, economic espionage involves state action that tries to take the trade secrets of foreign companies (Brown, 2016). As a result, with the absence of international law that regulates cyber economic espionage, President Obama's administration has taken several measures to handle China's commercial cyber spying, especially through diplomacy and cooperation. In this research, the United States strategy to counter Chinese cyber economic espionage will be analyzed using the concept of cyber diplomacy and secondary data collection methods to answer the research question: "How is the effectiveness of the United States' diplomacy process to counter the economic cyber espionage comes from China during the year 2010-2015?"

Cyber diplomacy is a concept that can provide a deeper understanding of what happens between states amidst the emanating cyber security issues in international relations studies on the era of cyberspace, in which cyber diplomacy is being used as a foreign policy tool. According to Barrinha & Renard (2017), cyber diplomacy means "diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to cyberspace." The interests here refer to the national cyberspace and cybersecurity strategies that frequently lead to the diplomatic

agenda. On the other hand, Kumar (2022) has given a more simple definition of cyber diplomacy by defining it as “the use of diplomatic tools and diplomatic thinking to resolve issues arising in cyberspace.” This concept is able to demonstrate interactions in the world system that is growing to be more complicated and multifold since cyberspace has turned into another contested area (Hodžić & Astrov, 2017), which make diplomatic functions are needed to maintain peace and build mutual trust among stakeholders (Barrinha & Renard, 2017).

In general, cyber diplomacy addresses foreign agenda that includes cybercrime management, cybersecurity, international freedom, internet governance, and trust-building (Iswardhana, 2021). The strong demand for international commitment and collaboration in the political decisions regarding cyberspace has made cooperation become an important dimension for diplomatic activity in the cyber domain to conclude diplomatic engagements and multi-level agreements (Danca, 2015). In regard to that, there is a wide range of diplomatic agendas engaged in cyber diplomacy such as fostering dialogue and communication between state and non-state actors, developing global norms, promoting national interests, and preventing cyber arms race (Manantan, 2021). With the use of negotiations, cyber diplomacy will be able to fill the gaps between countries when cyberwar or a series of cyberattacks happens in order to prevent the conflict from escalating into economic devastation or deadly conflict (Kumar, 2022).

This research decided to use a secondary data collection methodology in order to gather all existing relevant data information that can be utilized to analyze and answer the research problem that is being highlighted. According to the previous studies from Hox & Boeije (2005), primary data previously collected by other researchers or for other purposes aside from research is possible to be used as secondary data based on the virtue that the data itself is being archived and made available. Secondary data collection methodology is being used for this research due to the conceptual and substantive reasons by considering the actors involved, location, and the time period that is taken. As has also been mentioned by Chivaka (2018), secondary data could be the only available data that can be relied on to solve some research problems. The main sources of secondary data that will be used for this research, will mostly come from previous publications, such as written books, journals, news, government publications and other credible websites. Later on, all the data that have been collected will be compiled together and examined through further discussion in order to reach the final conclusion regarding the effectiveness of the United States' actions in combating Chinese economic cyber espionage that has threatened the country’s national security.

The Accusation of China's Cyber Espionage

a. China Cyber Capability

China has kept developing its potential in cyber capabilities for years until it can become a country with strong cyber power that has been widely recognized. Since China does not want to rely only on military applications, this country regards computer network operations to be a strategic significance that is broadly implemented to help the long-term strategies for the country's national development (Krekel, Adams, & Bakos, 2012). China has executed a broad technology development plan through grant programs for the development of cyber capabilities. Commercial IT companies along with civilian and military universities that held research related to computer network operations have actively received funds grant programs from the Chinese government, and at least 50 civilian universities that conducted nationwide research about information security are given one or more of the main national-level high technology grant programs (Ibid.). Nevertheless, Chinese advancement in computer network operation also poses threats to the United States national security.

Some analysts argue that the desire of China to have the global-power status is what makes it possible for this country to have the most extensive and aggressive cyber warfare power in the world, as can be seen from the authoritative Chinese writings which showed that cyber warfare is used as an instrument to balancing those overwhelming power, especially the United States (Hjortdal, 2011). The reason beyond it is because China believed that the United States is a revisionist power that would like to limit the political influence of China and put China's interests in harm (Iasiello, 2016). As a result, instead of trying to deter the power of the United States, China more likely aims to strengthen its power through the conduct of cyber operations in order to extract information related to the United States' economic, diplomatic, and defence industrial base sectors that support the national defence programs. China also aggressively seeks for the trade secrets of foreign companies as well as intervenes to support its domestic companies in competing with foreign competitors. Data even showed that from all the total of open economic espionage and trade secret theft investigations in the United States, China contributes around 50% to 80% of it (Reid, 2016).

Aside from that, the 12th Five-Year Plan (2011–2015) that was drafted by the People's Liberation Army (PLA) together with the central government of China has prominently reflected most of the common targets of Chinese cyber espionage. China wrote seven industries that were prioritized to be developed in the five years economic plan where

coincidentally the United States has been known to be the leader and innovator of those industries. The industries mentioned in the Five Year Plan are "new energy (nuclear, wind, solar power), energy conservation and environmental protection (energy reduction targets), biotechnology (drugs and medical devices), new materials (rare earths and high-end semiconductors), new IT (broadband networks, Internet security infrastructure, network convergence), high-end equipment manufacturing (aerospace and telecom equipment), and clean energy vehicles" (Iasiello, 2016). Therefore, the link between the sector industries in the United States that are the targets of cyber attacks with the strategic industries that China would like to be developed can be correlated easily (Ibid.).

b. Cyber Espionage in the United States Committed by China

The advent of economic cyber espionage conducted by China to gain commercial advantages for its domestic companies has worsened the long-existing issue of Chinese violation toward American intellectual property and poses a complex problem for the United States' national security. The issue of cyber spying began to attract media attention and become a great concern for the American government, after Google as an American big technological company made an announcement in January 2010 that it became a victim of a sophisticated attack, originating from China, that targeted Google's corporate infrastructure. David Drummond, Google's Senior Vice President of Corporate Development and its Chief Legal Officer, stated that the attack, which was detected in mid-December 2009, has led to Google's intellectual property theft (Hartnett, 2011). The attackers were targeting the Gmail accounts of Chinese human rights activists and dissidents as the main goal (Nakashima, 2013), and managed to steal valuable source codes which contain instructions related to computer programmers to develop software programs that can bring insights regarding security weaknesses as well as give economic advantages (Segal, 2013). According to the report from VeriSign Defence, the culprit behind the attacks on Google was the Chinese Government, which involved two Chinese educational institutions, Lanxiang Vocational School and Shanghai Jiaotong University (Hjortdal, 2011). In response to this economic cyber espionage issue, Google threatened to remove the censorship of certain items from its Chinese network and shifted its Chinese internet activities focus to Hong Kong after China accused Google of evading Chinese law (Thomas, 2010).

Aside from Google, several other companies are also reported to have received cyber attacks from China. It turned out that the negotiation strategies and financial information of firms in the energy, finance, and legal

sectors, as well as industry groups also become the target of Chinese hackers (Segal, 2013). Following the argument that has been said for a long time by many cyber-observers, actually China was conducting massive electronic espionage operations around the world, targeting US military intelligence, multinational corporate research, and political dissidents (Hartnett, 2011). At first, Google reported that there were at least 20 other companies that were victims of cyber espionage, however, industry investigations then found that the hackers had attacked 34 American-based technology firms (Read, 2013). Those companies that reported being attacked by the hackers were including Adobe Systems, California, software maker CyberSitter Dow Chemical, Disney, DuPont, General Electric, General Dynamics, the law firm Gipson Hoffman & Pancione, Johnson & Johnson, Juniper Networks, the law firm King & Spalding, Northrop Grumman, Rackspace Hosting, the Santa Barbara, Sony, and Yahoo (Segal, 2013). In describing how invasive the attacks were, Alan Paller, the director of the SANS Institute in Bethesda, Maryland, even said that the probability for the 25 biggest companies in California not to be entirely compromised by China is almost none (Thomas, 2010). Moreover, some experts also estimate that the United States has lost around 0.1% to 0.5% of the gross domestic product, or $25 billion to $100 billion due to cyber espionage (Nakashima, 2013).

Amidst these rising concerns about China's economic cyber espionage, several reports were released and noted various data related to Chinese cyber activities. These are including the report of the Federal Bureau of Investigation (FBI) that leaked, which claimed that China had developed its cyber army that was made up of 150,000 private sector spies and 30,000 military cyber spies (Hjortdal, 2011). The Wall Street Journal also reported in December 2011 that Chinese cyber espionage is mostly sponsored by China military, and the confidential report by the Defense Science Board that described by the Washington Post in May 2013 was stated that cyber intruders have managed to access over 24 designs of the United States weapon system (Reid, 2016). The Washington Post as well reported that according to the National Intelligence Estimate, China is the most aggressive country that is attempting to penetrate into the computer systems of American institutions and corporations with the purpose to get access to data that can be used for commercial gain through a massive, sustained cyber-espionage campaign (Cate, 2015). Furthermore, in the United States, China is estimated to have owned more than 3,000 front companies that operate where some of them have the sole purpose of only facilitating technology transfer to China (Reid, 2016).

Other than that, a security company Mandiant also released a comprehensive report in February 2013 that identified the involvement of

Chinese military units in cyber spying. According to the Mandiant report, the Chinese government has supported and given funding to more than twenty Advanced Persistent Threat (APT) groups that operating from China, in which one of these groups refers to as APT1 has become one of the most prolific cyber espionage groups that are able to steal hundreds of terabytes of data from at least 141 private corporations over twenty industries (Lee, 2013). In the report, it stated that beside from the minutes of board and executive meetings and the senior employees' email content, "electronic data on product development and use, test results, system designs and product manuals, manufacturing procedures, business and strategy plans, negotiation and pricing strategies, and details of joint ventures and collaboration with other entities" are among the materials stolen from US industry (Ibid.). Eventually, the publication of this document has made the United States government become more active in facing economic cyber espionage from China after previously tending to be more cautious and avoid unequivocally pointing to China due to the origins of some activities in the cyber domain that are hard to identify.

For senior United States government officials, including President Obama, the release of the PLA Unit 61398 activities report from Mandiant has become a turning point for them to address the Chinese cyber espionage issue publicly. In March 2013, not long after the report was published, Thomas Donilon, the United States National Security Advisor, mentioned that "…businesses are speaking out about their serious concerns about sophisticated targeted theft of confidential business information and proprietary information through cyber intrusions emanating from China" (The White House, 2013). However, the government of China has denied the allegations written in the report, even though the buildings mentioned by Mandiant were vacated soon after the document's release (Inkster, 2016). The issue between the United States and China was then getting heated up after five members of the Chinese military were arrested by the United States Department of Justice in May 2014 for infiltrating corporate computer networks and stealing a large American company's trade secrets.

Conflict Settlement

a. China's Responses

As can be predicted, China dismissed all the accusations that point out the involvement of the Chinese government in the cyber economic espionage case in the United States. This includes the allegation from Google that China regards it as groundless. Even in response to Google's

threat that would like to remove censorship after being attacked by the hackers that believed originating from China, the Chinese government just told Google to adhere to China's laws and regulations without mentioning the reasons behind Google's decision (Thomas, 2010). Nevertheless, as in this period, the image of China was framed as an antagonistic cyber presence, and now China's response has evolved. The government's response toward the cyber economic espionage accusations is always consistent by invariably denying all the charges that do not have sound proof. The official statements from China's Prime Minister, the Ministry of Defense, and the Ministry of Foreign Affairs (MFA) are all emphasizing that the attacks are not carried out by China, that China is a victim of cyber-crime activity instead of a perpetrator, and that hacking is considered illegal under China's laws (Iasiello, 2016). However, the Chinese government was reluctant to give confirmation regarding whether they sponsored or participated in economic cyber espionage activities or not. China's Ministry of Defense rather accused the Mandiant report was still lacking on technical and legal grounds by stating that the provided evidence from linking the IP and building addresses to specific hackers did not have a technical basis (Xiaofeng, 2016).

Furthermore, China's response in facing the economic cyber espionage accusation was getting more assertive, especially after Edward Snowden, the former National Security Agency (NSA) contractor, leaked highly classified documents in 2013 that revealed the United States' global spying efforts. This information that was released prior to the US-China summit also exposed the NSA's actions related to cyber exploitation that were designed to enhance surveillance, conduct cyberattacks, and interfere with internet transactions (Cate, 2015). The documents reported that the United States was not only hacking China's largest fibre-optic submarine cable network, monitoring communications of Chinese leaders, and attacking the data centre of Tsinghua University, but also actively invaded the internal network system of China's big telecommunication company Huawei as the primary target (Ibid.). In regards to this, Chinese MFA harshly criticized the United States government that they have ulterior motives and double standards, as well as becoming a robber that acts like a cop (Xiaofeng, 2016). At this point, China was no longer trying to deflect the accusations as an economic cyber espionage perpetrator, but to reverse the situation by pointing fingers at the United States government. In March 2014, the United States was even identified as the leading source of intrusion activity against China's computers by the Chinese National Computer Emergency Response Team (Iasiello, 2016).

Hence, it was hard for the United States to deny its spying activities on commercial companies due to the Snowden revelations, and instead, the United States government decided to reframe its formulation on cyber espionage by limiting what can be done with the espionage results rather than just enjoining specific surveillance targets. This is represented in the claim from the head of the United States Justice Department's National Security Division, John Carlin, who defends that "the United States spying on foreign companies is qualitatively different than what the Chinese are doing, because the United States doesn't share the fruits of its espionage directly with companies, the way China does" (Harris, 2014). Yet, with the revelations of cyber operations that the United States conducted against Huawei, other networks in China, and elsewhere, that claim was doubted and considered as a trite. The outrage that comes from both the United States' allies and adversaries as a result of the Snowden scandal has led to the fallen public image of the United States (Iasiello, 2016). The former Special Counsel to the Department of Defense during the George W. Bush administration, Jack Goldsmith, also argues that "the Huawei revelations are devastating rebuttals to hypocritical U.S. complaints about Chinese penetration of U.S. networks, and also make USG protestations about not stealing intellectual property to help U.S. firms' competitiveness seem like the self-serving hairsplitting that it is" (Goldsmith, 2014). In this situation, China continues to portray itself as a victim of cybercrime while also showing its desire to have mutual cyber cooperation with the United States.

Nonetheless, the tension between the United States and China was further escalated due to the United States indictment of Chinese military officers. China's MFA criticize that this accusation was made based on fabricated facts, was violating the fundamental norms in international relations, was jeopardizing the mutual trust and cooperation between both countries, and only aims to promote the United States' hegemony in cyberspace (Xiaofeng, 2016). China's Foreign Ministry even announced the suspension of the China-US Cyber Working Group by claiming that the United States lacked sincerity in solving the cyber security issues through dialogue (Yin, 2014). Until finally this issue was able to find a turning point in 2015 through a bilateral agreement between the United States and China regarding cybersecurity matters, which will be explained further in the next part. After the agreement was made, China authorities did not hesitate to detain its own citizens whom the United States identified as hackers to demonstrate its commitment. In addition to this, together with Japan, Malaysia, and South Korea, the Chinese government has been actively participating in cyber security discussions, as well as a series of no-hack

pacts that culminated in the G20 agreement in November 2015 to forbid cyber-enabled commercial espionage (Iasiello, 2016).

b. The United States Diplomatic Responses

Following the issue of economic cyber espionage involving intellectual property theft that has been heating up since January 2010, the United States government under the Obama administration decided to place this problem as their special concern since it put the country's national security at risk. This concern was as well expressed in President Barack Obama's Cyberspace Policy Review in 2011, which noted that some of the most critical challenges for national security and the economy in this current century are the impact of cybersecurity threats (Lieberthal & Singer, 2012). Therefore, the United States government has tried various ways to fight against online trade secret theft, including strengthening its partnerships through diplomacy, as written in the U.S. *International Strategy for Cyberspace* document that was published in May 2011. Two years later, in 2013, the administration also released five new strategic actions to mitigate trade secret theft through (1) increasing diplomatic engagement together with countries that share the same concerns; (2) supporting businesses to exchange their best practices in protecting trade secret; (3) encouraging domestic law enforcement operations; (4) improving the state's legislation; and (5) raising public awareness of trade secret theft (Espinel, 2013). With this new strategy, the diplomatic process and legal agreements will be greatly used to increase trade secret protection as its priority.

One of the uses of diplomacy and legal agreements was shown in the execution of the strategy to sustain and coordinate international involvement with trading partners, which led to the expansion of its cyber espionage policy to encompass the use of trade tools. Those trade policy tools were utilized for strengthening international enforcement in counter trade secret theft to reduce unfair competition toward American businesses (Fidler, 2013). Furthermore, the implementation of this strategy will require "deeper cooperation with like-minded trading partners, seeking new provisions on trade secret protections in trade negotiations (e.g., the Trans-Pacific Partnership Agreement), and using the Special 301 priority watch list process to gather and act upon information about the adequacy and effectiveness of trade secret protection by U.S. trading partners" (Ibid.). This strategy became more specific after the then-new ambassador to China, Max Baucus, gave his speech in June 2014 by arguing that China's criminal behaviour has been in contrast with its commitments in the World Trade Organization (WTO) (Malawer, 2014). China, however, disagrees with this statement since it has a different argument. This is because, from China's

perspective, economic cyber espionage was a quasi-legitimate way because China considers economic development as part of national security and the Trade-Related Aspects of Intellectual Property Rights (TRIPS) was never conceived of as having an extraterritorial dimension (Inkster, 2016). Despite that, in facing the cyber issue that threatened the United States' national security and companies' global competitiveness, bringing an action in the WTO can be regarded as a proactive way to leverage the existing institutions and agreements since some cyber threats can only be addressed through indirect action using agreements on trade or law enforcement cooperation (Ibid.).

On the other hand, still in the use of the diplomatic process, the State Department of the United States also brought this economic cyber espionage issue to be part of its strategic security dialogue with China in order to give diplomatic and political pressure on the Chinese government. This issue was enhanced as a major problem that was discussed in every bilateral dialogue between China and the United States, including during the strategic and economic dialogue (S&ED) as well as in the talks on defence, judicial, and trade affairs (Xiaofeng, 2016). The presidents from both countries had their first dialogue on cyber security when commercial cyber espionage was incorporated into the Strategic and Economic Dialogue on 8 June 2013 as one of the two leading issues (Xu & Lu, 2021). A month later, in July 2013, the military departments of China and the United States agreed to establish China–U.S. Cyber Working Group (CWG) to be their main platform to have bilateral dialogue related to cyber issues and held their first meeting (Ibid.). However, this problem escalated after the United States government decided to take judicial measures against the perpetrators of economic cyber espionage due to the diplomatic pressure that failed to reach the expected outcomes. The government charged five Chinese military officers on 19 May 2014 with the indictment of computer hacking, economic espionage and other infringements that targeted six victims in U.S. metals, nuclear power and solar products industries (Xiaofeng, 2016). Meanwhile, the Chinese government that did not accept those accusations demanded the United States to withdraw the case and suspended the dialogue in China–U.S. Cyber Security Working Group, and at that moment the cyber dialogue between China and the United States has fallen into a long deadlock.

In 2015, the cyber espionage issue was getting even worse. As a result, the United States began to exercise economic sanctions for the perpetrator of economic cyber espionage, following the release of a presidential executive order entitled “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities” in April 2015, which applies to individuals and not foreign states (*Exec. Order*

2015). Nevertheless, the United States was considering giving sanctions for individuals or entities that benefit from cyber theft after the U.S. Office of Personnel Management announced in June 2015 that its computer networks had been infiltrated, in which the Social Security numbers and other personal data of over 21 million Americans had been stolen (Xu & Lu, 2021). The plan to give sanctions on China was however held off due to the concern that this action would harm its relationship with China (Sevastopulo & Dyer, 2015). Fortunately, China and the United States managed to reach an agreement during Chinese President Xi Jinping's visit to the United States in September 2015 and committed that both governments will not conduct economic cyber espionage. In more detail, there are four points that have been agreed upon by the leaders of these two countries, which are: "(1) both countries will respond in a timely manner to requests for information and assistance related to the pernicious cyber activity; (2) neither country will participate or sponsor cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors; (3) China and the United States will strive to identify and endorse proper norms of state behaviour in cyberspace; (4) the two leaders established a high-level working group to deter the spread of illegal cyber activity, and a hotline to address serious security issues" (Hufbauer & Jung, 2015).

Subsequently, the cyber agreements between China and the United States have brought positive impacts in declining the number of cyber crimes in the final years of President Obama's administration. Compared to the number of economic cyber espionage operations since May 2014 when five China military officers were charged, the number of cases had been declining not long after China's state visit (Inkster, 2016). Moreover, the number of cyber criminals that were detained and prosecuted in China increased in 2015 (Ibid.). In addition, the report from FireEye that was released in June 2016 also showed that there was a decline in the number of networks compromised by Chinese hacker groups, from 60 in February 2013 to less than 10 by May 2016 (Segal, 2016). At this point, the steps taken by the United States, especially through the use of cyber diplomacy to build cooperation against economic cyber espionage issues that threatened national security, were such a remarkable achievement.

Conclusion

The international system that becomes more complicated after entering the era of cyberspace has led to the growing need for international cooperation which

can be achieved through the use of diplomacy activity in the cyber domain. Even countries with strong power, such as China and the United States, were no exception. In order to avoid the escalation of the cyber conflict, China and the United States are required to continue pursuing mutual cooperation, as can be seen during the economic cyber espionage conflict between China and the United States in 2010 - 2015. In resolving this issue, the United States was able to push China into making a bilateral agreement through the use of cyber diplomacy as part of its foreign policy strategies and avoided the plan to impose sanctions on China. The diplomacy process of the United States itself was represented in its effort to cooperate with the trading partners for trade secret protections, bringing up this issue to the WTO, and the bilateral dialogues journey with China. This issue then closed with China's massive detention of economic espionage criminals and the reduction of economic cyber espionage cases in the United States. Therefore, it can be said that the practice of cyber diplomacy that the United States government conducts to resolve this cyber issue is relatively effective considering the final outcomes of it. Moreover, at the end of the day, the occurrence of this issue has made both the United States and China realize the importance of a diplomatic approach to address the emerging cyber security issues together with the other states.

References

Banks, W. C. (2017). Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage. *Emory Law Journal*, *66*(2), 513–525. Retrieved from https://scholarlycommons.law.emory.edu/elj/vol66/iss3/3 .

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4-5), 353–364. https://doi.org/10.1080/23340460.2017.1414924

Brown, G. D. (2016). Spying and Fighting in Cyberspace: What is Which? *Journal of National Security Law & Policy*, *8*(3), 621–635. Retrieved from https://jnslp.com/2016/03/29/spying-fighting-cyberspace/.

Buchan, R. (2019). Introduction. In *Cyber Espionage and International Law* (pp. 1–12). introduction, Hart. Retrieved from https://lccn.loc.gov/2018034245.

Cate, F. H. (2015). China and Information Security Threats. In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (pp. 297–332). Oxford University Press. https://doi.org/https://doi.org/10.1093/acprof:oso/9780190201265.001.0001

Chivaka, R. (2018). *Secondary Data Analysis*, 1–5. Retrieved from https://www.researchgate.net/publication/327060808_secondary_data_analysis.

Danca, D. (2015). Cyber Diplomacy – A New Component of Foreign Policy. *Journal of Law and Administrative Sciences*, (3), 91–97. Retrieved from https://www.ceeol.com/search/article-detail?id=443948.

Espinel, V. (2013, February 20). *Launch of the Administration's Strategy to Mitigate the Theft of U.S. Trade Secrets*. Retrieved December 4, 2022, from

https://obamawhitehouse.archives.gov/blog/2013/02/20/launch-administration-s-strategy-mitigate-theft-us-trade-secrets

Exec. Order No. 13694, 3 C.F.R. 18077 (2015).

FBI. (2016, June 13). *What is "economic espionage"?* Retrieved November 8, 2022, from https://www.fbi.gov/about/faqs/what-is-economic-espionage

Fidler, D. P. (2013). *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies*, *17*(10). Retrieved from https://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving.

Goldsmith, J. (2014, March 22). *The NYT on NSA's Huawei Penetration [UPDATED]*. Retrieved December 4, 2022, from https://www.lawfareblog.com/nyt-nsas-huawei-penetration-updated

Handford, E. (2014). *The Cold War of Cyber Espionage*, *20*(1), 22–25. Retrieved from http://lawecommons.luc.edu/pilr.

Harris, S. (2014, May 27). *Exclusive: Inside the FBI's fight against Chinese Cyber-Espionage*. Retrieved December 4, 2022, from https://foreignpolicy.com/2014/05/27/exclusive-inside-the-fbis-fight-against-chinese-cyber-espionage/

Hartnett, S. J. (2011). Google and the "Twisted Cyber Spy" Affair: US–Chinese Communication in an Age of Globalization. *Quarterly Journal of Speech*, *97*(4), 411–434. https://doi.org/10.1080/00335630.2011.608705

Hjortdal, M. (2011). China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security*, *4*(2), 1–24. https://doi.org/10.5038/1944-0472.4.2.1

Hodžić, N., & Astrov, A. V. (2017). *Cyber Diplomacy: Framing the Transformation* (thesis). Central European University, Budapest. Retrieved from https://www.etd.ceu.edu/2017/hodzic_nejra.pdf.

Hox, J. J., & Boeije, H. R. (2005). Data Collection, Primary vs. Secondary. *Encyclopedia of Social Measurement*, 593–599. https://doi.org/10.1016/b0-12-369398-5/00041-4

Hufbauer, G. C., & Jung, E. (2015, September 29). *What Obama did and did not accomplish in cyber-espionage talks with Xi*. Retrieved December 4, 2022, from https://www.piie.com/blogs/china-economic-watch/what-obama-did-and-did-not-accomplish-cyber-espionage-talks-xi

Iasiello, E. (2016). China's Three Warfares Strategy Mitigates Fallout From Cyber Espionage Activities. *Journal of Strategic Security*, *9*(2), 47–71. https://doi.org/10.5038/1944-0472.9.2.1489

Inkster, N. (2016). Cyber Espionage. *Adelphi Series*, *55*(456), 51–82. https://doi.org/10.1080/19445571.2015.1181443

Iswardhana, M. R. (2021). Cyber Diplomacy And Protection Measures Against Threats Of Information Communication Technology In Indonesia. *Journal of Islamic World and Politics*, *5*(2), 343–367. https://doi.org/10.18196/jiwp.v5i2.12242

Krekel, B. A., Adams, P., & Bakos, G. (2012). *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. Northrop Grumman Corp. Retrieved from

https://www.uscc.gov/research/occupying-information-high-ground-chinese-capabilities-computer-network-operations-and.

Kumar, A. (2022). Cyber Diplomacy - The Concept, Evolution and Its Applicability. *International Journal of Cyber Diplomacy*, *3*, 23–32. https://doi.org/10.54852/ijcd.v3y202203

Lee, J. (2013). CYBER KLEPTOMANIACS: Why China Steals Our Secrets. *World Affairs*, *176*(3), 73–79. Retrieved from https://www.jstor.org/stable/43555412.

Libicki, M. (2017). The Coming of Cyber Espionage Norms. *2017 9th International Conference on Cyber Conflict (CyCon)*, 1–17. https://doi.org/10.23919/cycon.2017.8240325

Lieberthal, K. G., & Singer, P. W. (2012). (rep.). *Cybersecurity and U.S.-China Relations*. Brookings. Retrieved from https://www.brookings.edu/research/cybersecurity-and-u-s-china-relations/.

Malawer, S. S. (2014). Confronting Chinese Economic Cyber Espionage With WTO Litigation. *New York Law Journal*, (120), 1–5. Retrieved from http://www.newyorklawjournal.com/id=1202712784205/Confronting-Chinese-Economic-Cyber-Espionage-With-WTO-Litigation#ixzz3MfIKeTXb.

Manantan, M. B. F. (2021, November 10). *Defining Cyber Diplomacy*. Retrieved December 6, 2022, from https://www.internationalaffairs.org.au/australianoutlook/defining-cyber-diplomacy/

Nakashima, E. (2013, February 10). *U.S. said to be target of massive cyber-espionage campaign*. Retrieved December 2, 2022, from https://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html

O'Hara, G. (2010). Cyber-Espionage: A Growing Threat to the American Economy. *CommLaw Conspectus: Journal of Communications Law and Technology Policy*, *19*, 241–275. Retrieved from https://scholarship.law.edu/commlaw/vol19/iss1/9.

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

Read, O. (2013). How the 2010 Attack on Google Changed the US Government's Threat Perception of Economic Cyber Espionage. *Cyberspace and International Relations*, 203–230. https://doi.org/10.1007/978-3-642-37481-4_12

Reid, M. (2016). *A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat?*, *70*(3), 757–829. Retrieved from https://repository.law.miami.edu/umlr/vol70/iss3/5.

Segal, A. (2013). The code not taken: China, the United States, and the future of Cyber Espionage. *Bulletin of the Atomic Scientists*, *69*(5), 38–45. https://doi.org/10.1177/0096340213501344

Segal, A. (2016, September 28). *The U.S.-China Cyber Espionage Deal One Year Later*. Retrieved December 4, 2022, from https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later

Sevastopulo, D., & Dyer, G. (2015, September 25). *Obama and Xi in deal on cyber espionage*. Retrieved December 4, 2022, from https://www.ft.com/content/0dbcab36-63be-11e5-a28b-50226830d644

The White House. (2013, March 11). *Remarks By Tom Donilon, National Security Advisor to the President: "The United States and the Asia-Pacific in 2013"*. Retrieved December 4, 2022, from https://obamawhitehouse.archives.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisor-president-united-states-an

Thomas, T. L. (2010). Google Confronts China's "Three Warfares." *The US Army War College Quarterly: Parameters*, *40*(2), 101–113. https://doi.org/10.55540/0031-1723.2528

Xiaofeng, W. (2016). China's Alternative Roles in Countering International Economic Cyber Espionage. *China Quarterly of International Strategic Studies*, *02*(04), 549–568. https://doi.org/10.1142/s2377740016500251

Xu, M., & Lu, C. (2021). China–U.S. cyber-crisis management. *China International Strategy Review*, *3*(1), 97–114. https://doi.org/10.1007/s42533-021-00079-7

Yin, C. (2014, May 20). *Suspension of cyber group will affect Sino-US talks*. Retrieved December 4, 2022, from https://www.chinadaily.com.cn/world/2014-05/20/content_17525683.htm