CHINESE ESPIONAGE ACTIVITIES AGAINST THE UNITED STATES MILITARY INDUSTRY

Ghina Arindiya
International Relations Study Program, Indonesian Computer University, Bandung, Indonesia

Dewi Triwahyuni
International Relations Study Program, Indonesian Computer University, Bandung, Indonesia

ABSTRACT

This research aims to analyze China's espionage activities against the United States, especially in the military industry. In analyzing the case the author uses the concepts of the Action-Reaction Model and Information War. The espionage conflict between the US and China is influenced by the proximity and complexity of political, technological and strategic factors. The collection technique was carried out through literature study and then analyzed using qualitative methods. The results of this research show that espionage has a major influence on the complexity of cyber security. Final conclusions about Chinese espionage against America will depend largely on the actual evidence available, and these assessments are often carried out in great secrecy. However, espionage conflict is a serious problem that requires a coordinated and strategic response from the government and related institutions

Keywords: China, Cyberwar, Espionage, Realist Theory, United States

INTRODUCTION

The development of information technology has had a major impact on various aspects of life, including among society and state institutions. It is true that information technology has brought ease in the exchange of information and communication. In technological advances in this modern era, every element in the state is obliged to maintain sovereignty, security in every aspect such as in cyberspace which is a new domain or part in maintaining the survival of the state. For this reason, some countries have realized how vital the cyber world is in the life of the nation and state. The progress of cyberspace cannot be separated by the development of the internet because in general people know the virtual world from the internet. Internet stands for interconnected network, which is a device that can be connected through a network system. (New Media Institute, 2017) The Internet was originally created for military and educational purposes in the United States.

The function of this technology is used not only among the community but in state institutions, military and so on to take advantage of existing advances. This progress has both good and bad effects, both facilitate communication, and find information but even so many bad things can be caused such as misuse such as fraud, hacking, and other Cyberspace attacks. Cyberspace in Indonesian is cyberspace, a world where there is a two-way or one-way relationship connected through a computer network. According to Perry Barlow and Bruce Sterling in their book The Hacker: Online Crackdown and Disorder On The Electronic Frontier, the two characters mentioned that "Cyberspace is an invisible space" (Barlow & Sterling, 1992). An understanding of the concept of cyberspace is also important, as it refers to the environment in which digital interactions occur, and where cyber security risks often arise. By understanding and recognizing the importance of cybersecurity, communities and institutions can be better prepared to face the challenges associated with the use of information technology in everyday life. Cyberattacks can cause significant financial losses to companies and financial institutions. For example, hacking attacks or theft of financial data that can harm the company and its customers. Governments are often the target of cyberattacks aimed at stealing classified data, military information, or other strategic information. This kind of data theft can harm a country's national interests. Cyberattacks can be aimed directly at critical infrastructure such as electrical systems, transportation systems, or healthcare infrastructure. Such attacks can have devastating repercussions on people's daily lives and the stability of the country.

The beginning of cyberspace development in the US can be traced back to the ARPANET (Advanced Research Projects Agency Network) which was built in 1969 by the US Department of Defense. ARPANET is designed to be a robust and reliable communication network between research and educational institutions. This was an important milestone in the development of the modern internet. In the early 1990s, the Internet began to experience significant commercialization in the United States. This happened simultaneously with the invention of the World Wide Web by Tim Berners-Lee in 1989. Companies are beginning to realize the potential of the internet as a platform for business and commercial interaction. The dot-com boom period of the late 1990s and early 2000s created a huge surge in internet usage in the US. Many new internet companies have sprung up, and investors are speculating aggressively in technology-related stock markets. Despite the significant bankruptcy of the industry in 2000 (dot-com bust), the foundation of the internet economy continues to grow. As the Internet grew, the U.S. government began to develop regulations and policies related to security, privacy, and consumer protection in cyberspace. Examples include the Freedom of Information Act (FOIA) of 1966, the Electronic Government Act (E-Government Act) of 2002, and others. The proliferation of social media such as Facebook, Twitter, and LinkedIn, as well as e-commerce platforms such as Amazon and eBay, has significantly changed the way Americans interact, shop, and do business. This has created a thriving digital economy. Along with technological developments, cyber security threats are also increasing in the United States. Cyberattacks such as hacking, data theft, and malware attacks have become a serious challenge for governments, companies, and individuals in the US, prompting increased investment in cybersecurity.

Cyberspace has become a significant space in state and military affairs. The growth and development of information technology has changed the overall security landscape, with new issues emerging in the context of national security and defense. One of the main challenges faced by countries is cyber espionage (Sindonews, 2017). It is an activity carried out by other countries or entities to steal confidential or strategic information from other countries through cyber attacks. Cyber espionage can include the theft of military data, trade secrets, or other sensitive information that can harm a country's national security and economic interests. In addition to espionage, there are also other threats in cyberspace that can affect state and military affairs, such as cyber attacks aimed at disrupting critical infrastructure, sabotage, propaganda, and others. Therefore, countries are seriously paying attention to protecting their critical infrastructure from cyberattacks, as well as improving the ability of cyber defenses to cope with such threats. This demonstrates the importance of countries to develop effective cyber security policies and strategies, cooperate internationally in combating cyber threats, and invest sufficient resources in building strong cyber defense capabilities.

China and the United States have been considered major actors in the cybersecurity realm due to their technological strength, vast resources, and strong political, military, and economic motivations. In this context, cyberattacks can be part of the strategies used by both countries to achieve their goals, be it to gain military advantage, secure classified information, damage opposing infrastructure, or influence political processes and public opinion at the domestic and international levels. Conflicts in the cybersecurity domain are not unique to China and the United States, but also involve various other countries and non-state actors such as hacker groups or criminal organizations. This dynamic creates complex challenges in maintaining cybersecurity globally.

There have been several previous studies examining similar themes. The first research titled “Analysis of the United States' Motivation for Cybersecurity Cooperation with China" (Purwani, 2019). Researchers found similarities in researching, namely the analysis of the United States Cyber Security Cooperation with China, Another similarity found was about what cyber conflicts occurred between China and the United States. The difference is that researchers examined what attacks occurred after the 2015 cyber agreement. While the researcher above examined what cyber attacks occurred before the cyber agreement so that the United States and China re-established the Cyber Agreement in 2015.

Secondly, Raharjo (2016) conducted research entitled "United States Strategy in Facing China's Cyber Power Escalation 2011-2015". Researchers found similarities in examining how China conducts cyber attacks against the United States. Another similarity found is the response and reaction from America to cyber attacks carried out by China. The difference occurred in the period of research of the case. Researchers examined 2015 to 2021 which was after the "U.S.-China Cyber Agreement 2015". While the researcher above examined in the period 2011 to 2015, namely after the first agreement to the cyber agreement of the two superpowers.

The third reseach written by Prasetyo (2018) entitled "South Korea's Cyber Security Policy After the Cyber Attack by North Korea (2009-2014)". This research also analyzes cyber attacks between two countries and both carry the concept of cyber attack and cyber security as the main concept. The difference is that the researcher examined cyber attacks carried out by the Chinese state against the United States, while the researchers above examined attacks carried out by North Korea on South Korea. The Fourth research made by Aritonang (2019) entitled "Iran's Offensive Cyber Operations against the United States, Israel, and Saudi Arabia: Iran's Offensive Interests and Strategies". Researchers found similarities in researching, namely about cyber attacks against the United States. The difference is that the researcher examined cyber attacks carried out by the Chinese state, while the researchers above examined attacks carried out by the Iranian state.

Lastly, a study written by Ramadhanty (2018) with the title "Factors Causing the United States to Make China the Main Cyber Security Threat for the 2007-2014 Period". Researchers found similarities in the study, namely the concern of the United States feeling threatened by cyber attacks carried out by China. The difference is that researchers not only examined the factors that caused the United States to make China a cybersecurity threat, but also examined what attacks were carried out.

Enhancing cyber security by the United States in solidarity with its NATO allies, including Estonia as the cyber hub of NATO members, is an important step in confronting modern cyber threats. Through NATO, member states are committed to helping each other and protecting each other from any threat, including cyber threats. Estonia has taken center stage in the context of cyber security due to their experience in dealing with significant cyber attacks in 2007. This incident is an important lesson for the international community about the importance of cyber security and cooperation in dealing with such threats.

The publication of President Obama's International Strategy for Cyberspace in 2011 reflected U.S. awareness of the importance of addressing cyber threats that could threaten national security and sovereignty. The strategy is designed to protect U.S. critical infrastructure, strengthen cyber defenses, and work with other nations to combat cyber threats globally. Measures like these show that countries like the U.S. recognize the importance of cyber security as a new domain in national and international security. Through cooperation in organizations such as

NATO and policy strategies such as the International Strategy for Cyberspace, countries can jointly address cyber threats and build more resilient cyber security.

LITERATURE REVIEW

Espionage has long been a central aspect of statecraft and international relations, with both China and the United States engaging in extensive covert activities to gather intelligence and protect national interests. This literature review examines the evolving dynamics of espionage between China and the United States, focusing on key themes such as technological espionage, cyber espionage, and the impact on bilateral relations. Chinese espionage activities targeting the U.S. military industry have raised significant concerns among policymakers, security experts, and scholars alike. This literature review aims to provide an overview of the evolving landscape of Chinese espionage in the U.S. military sector, highlighting key themes, trends, and implications.

The history of Chinese espionage in the U.S. military industry dates back several decades, with notable cases such as the theft of nuclear secrets during the Cold War era (Dienstfrey, 2016). However, in recent years, the scale and sophistication of Chinese espionage activities targeting military technology and defense contractors have escalated, posing serious challenges to U.S. national security (Liang & Xiangsui, 2015).

China and the United States have been embroiled in a complex web of technological espionage, particularly in sectors such as defense, aerospace, and telecommunications. Scholars such as Smith (2018) have highlighted the systematic efforts of Chinese state-sponsored entities to acquire sensitive technology through both legal and illicit means. The theft of intellectual property and trade secrets has been a significant point of contention, leading to trade disputes and diplomatic tensions between the two powers. In response, the United States has implemented various measures, including export controls and sanctions, to counter Chinese technological espionage (Erickson & Rosen, 2020).

The emergence of cyberspace has transformed the landscape of espionage, offering new avenues for intelligence gathering and sabotage. Chinese state-backed hackers, in particular, have been implicated in numerous cyber intrusions targeting American government agencies, corporations, and critical infrastructure (Rid & Buchanan, 2019). The United States, for its part, has bolstered its cybersecurity defenses and retaliated with indictments and diplomatic pressure against Chinese hackers (Lindsay, 2020). However, the attribution and prosecution of cyber espionage remain challenging due to the covert nature of cyber operations and the difficulty of establishing clear accountability (Nye, 2019).

Chinese espionage operatives employ a variety of methods and tactics to infiltrate and gather sensitive information from the U.S. military industry. These include cyberattacks, insider threats, human intelligence operations, and exploitation of vulnerabilities in supply chains (Finklea, 2020). The use of cyber espionage, in particular, has emerged as a preferred tool for Chinese intelligence agencies to steal military-related technology and intellectual property (Rid & Buchanan, 2019).

The escalation of espionage activities between China and the United States has strained bilateral relations and exacerbated geopolitical tensions. Scholars such as Goldstein (2021) argue that mutual distrust and suspicion stemming from espionage have hindered cooperation on key issues such as trade, climate change, and regional security. Moreover, the perception of China as a pervasive espionage threat has fueled anti-Chinese sentiments in the United States and contributed to the adoption of more assertive policies, including the Indo-Pacific strategy and the Quadrilateral Security Dialogue (Quad) (Blanchette, 2020). The increasing frequency and sophistication of Chinese espionage pose significant challenges to U.S. national security and defense readiness. The theft of sensitive military technology and intellectual property not only undermines U.S. military superiority but also threatens the integrity of defense supply chains and erodes the competitiveness of U.S. defense contractors in the global market (Valero, 2019). Moreover, Chinese espionage activities in the U.S. military industry contribute to broader geopolitical

tensions between the two countries and complicate efforts to maintain strategic stability and deterrence in the Asia-Pacific region (Foust, 2017). In response to the growing threat of Chinese espionage, the U.S. government has implemented various countermeasures and initiatives to protect sensitive military information and mitigate vulnerabilities in the defense industrial base. These include strengthening cybersecurity defenses, enhancing counterintelligence efforts, imposing export controls on critical technologies, and prosecuting individuals and entities involved in espionage activities (Gertz, 2021).

METHODOLOGY

Qualitative research methods are used to understand phenomena in more depth, without ignoring the complexity and context in which they exist. Cyber security and cyber diplomacy cannot be separated from the political, economic and social contexts in which they emerge. A qualitative approach allows researchers to capture these contextual nuances, allowing for a more comprehensive interpretation of the issues at hand. The data collection technique used in this journal is literature study or literature review, where researchers analyze and evaluate various sources of previous research and other secondary data. Through collecting data from various sources such as journals, books, international treaty documents, and online news, researchers can gain rich and varied insights into cyber security and cyber diplomacy issues. The descriptive analysis approach allows the researcher to provide an in-depth description of cybersecurity issues in the United States and China. It involves analyzing and evaluating various sources of previous research and other secondary data to present a complete and detailed picture of the issue. The descriptive approach of this method allows researchers to describe the problem in sufficient detail, thereby providing a better understanding of cybersecurity issues in the US and China. By using a descriptive analysis approach and qualitative research methods, this research can make a significant contribution to understanding and overcoming the challenges of cyber security and cyber diplomacy at the national and international levels.

In this study, the author uses realism theory, action reaction model and Information Warfare. The action-reaction model is used to describe the dynamics of competition among international actors. In the context of this study, China's actions in conducting cyber espionage against the US military industry triggered a reaction from the US side. These reactions may include increased cybersecurity, tougher political rhetoric against China, or other measures aimed at protecting U.S. national security and responding to perceived threats. Information Warfare refers to the use of information and communication technology to achieve military, political, or economic objectives. In the context of this study, China's cyber espionage against the U.S. military industry can be viewed as part of Information Warfare, where China uses information technology to obtain sensitive information that can be used for its own strategic interests.

The theory of realism in the science of international relations emphasizes competition between states driven by national interests and relative power. In the context of this study, the theory of realism can be used to explain the competition between the US and China in the cyber domain. China is seen as a major U.S. competitor in gaining an edge in national security, and China's cyber espionage actions against the U.S. military industry could be interpreted as part of China's efforts to strengthen its position and threaten U.S. national security. Realism theory is used to describe the two competing countries, but the rivalry can threaten national security and survival for the US and in this case China which is a threat to national security for the US because it conducts cyber espionage against the US military industry.

RESULT AND DISCUSSION

The Internet has significantly changed the pattern of long-distance communication by providing various platforms and services such as email, instant messaging, social media, and video conferencing. It allows individuals and organizations to communicate quickly and efficiently without being limited by geographical boundaries. The Internet has a positive impact by facilitating easy communication and easy access to information. It enhances global connectivity, broadens horizons, enables collaboration, and empowers individuals in different areas of life. However, the internet also brings negative impacts such as hacking, espionage, and other criminal activities. Cyberattacks can harm individuals, companies, and even countries, with financial losses, personal data theft, and threats to national security. One of the main challenges in dealing with cyber threats is the difficulty in detecting such attacks. Perpetrators often use sophisticated techniques and tools to hide their tracks, making them difficult to identify and address. Cyberspace has evolved into two main layers, namely the Surface Web and the Deep Web, which are part of the World Wide Web (WWW). Surface Web includes publicly accessible websites, while Deep Web refers to content that is not indexed by search engines and requires authentication to access (CambiaResearch, 2016)) Surface Web is a part of the internet that can be accessed openly through search engines such as Google, Bing, and Yahoo. This includes websites commonly used in daily activities, such as news sites, social networks, e-commerce sites, and more. Users can easily find and access content on Surface Web without the need for special apps.

On the other hand, the Deep Web is a part of the internet that cannot be indexed by search engines and cannot be accessed openly. This includes sites that are not wanted or not allowed to be accessed by the public openly. While not all content on the Deep Web is illegal, many of these sites are used for activities of an illegal nature, such as online black markets, underground forums, and more. The Deep Web is difficult to track due to its anonymous use and often requires specialized applications such as TOR (The Onion Router) to access it.

The impact of these two layers is that although the Surface Web provides open and easy access for internet users, the Deep Web can be exploited by criminals to carry out illegal or harmful activities. Therefore, it is important to raise awareness about the risks and dangers associated with access to the Deep Web, as well as to develop effective security strategies to protect internet users from potential threats present in these two layers of the web. (Service Care Solution, 2016)

The economic revolution that began during the time of Deng Xiaoping did have a significant impact on China's economic development. Deng Xiaoping introduced economic reform policies that led to the opening of the Chinese market and the implementation of free market principles. China's joining the World Trade Organization (WTO) is an important step that expands market access for China and boosts its economic growth. The effect of these economic reforms is an increase in China's revenues and profits, which are then used to improve the defense sector and weapons production. China has succeeded in reducing dependence on imports of defense equipment by increasing domestic production. In fact, China has succeeded in becoming an exporter of defense equipment and weapons to other countries. According to a report from the Stockholm International Peace Research Institute, China's exports in the military sector increased significantly between 2011-2015, with an increase of 88%. This shows that China has successfully developed its defense industry and become a major player in the global arms market. (CNN Indonesia, 2016) China's rise as the world's third-largest arms exporter is indeed a serious concern for the United States. This shows that China has succeeded in rapidly and effectively developing its defense industry, as well as increasing its competitiveness in the global arms market. The emerging threat to the US is not only limited to economic competition in the arms market, but also involves security and strategic aspects. China, by being a major actor in the global arms market, has the potential to influence regional and global security dynamics. In addition, China's success in developing the defense industry could also threaten U.S. dominance in the military arena in some regions. China's alleged espionage against the US through the cyber domain is a concrete example of the intense rivalry between the two countries. This espionage can be interpreted as an attempt by China to gain a competitive advantage in the global arms market by accessing classified information or military technology in the possession of the US.

The shift in Chinese espionage motives from commercial focus to strategic goals does indeed reflect a shift in priorities and policy orientation under Xi Jinping's leadership. Since Xi Jinping took office as Chairman of the Central Military Commission in November 2012 and then as President in March 2013, there have been clear efforts to change the way China uses its resources, including in terms of intelligence gathering. This shift includes emphasizing China's long-term goals and strategic interests, while reducing the focus on more direct commercial gains. One of the measures taken is to reduce intelligence gathering conducted by some People's Liberation Army (PLA) units that are more focused on personal gain, such as stealing commercial technology for the benefit of private companies.

These measures are in line with the anti-corruption campaign promoted by Xi Jinping's government. The emphasis on transparency, accountability and more effective use of resources to achieve the country's strategic goals is part of a broader reform agenda in China under Xi Jinping's leadership. Nevertheless, despite the change in orientation in Chinese espionage motives, there is still evidence that commercial espionage remains part of Chinese spying activities. The data you provide indicate that most espionage incidents were reported after Xi Jinping took office, which may reflect a shift in focus on Chinese intelligence activities under his leadership. Therefore, it is important to continuously monitor and respond to Chinese espionage threats, both strategic and commercial in nature, as well as to strengthen cyber security systems and anti-espionage efforts at national and international levels.

The fact that the number of espionage incidents carried out by China far exceeds the number of incidents from other countries, even Russia, shows the significant level of spying activity carried out by China. This confirms that China is indeed one of the major players in the realm of cyber espionage at the international level. The long-term economic losses and impact on U.S. national security from Chinese espionage cannot be ignored. It is estimated that these losses run into billions of dollars, mainly from commercial espionage and technology theft. In addition, the theft of weapons technology and other sensitive information, such as nuclear weapons test data, poses a serious threat to U.S. national security and international stability. Over the past few years, China has increased the scope of its espionage activities to include various forms such as personal information theft (PII), political coercion, and influence operations. This suggests that China is not only aiming for economic gain or strategic advantage, but also to achieve broader political goals and global influence. The interests of the U.S. and other countries in countering Chinese espionage are critical. This requires joint efforts from the public and private sectors to improve cybersecurity, strengthen related laws and regulations, and strengthen international cooperation in tackling the threat of espionage. Only by confronting these threats together can countries protect their national interests and safeguard global cyber security.

The fact that espionage is the mode consistently chosen by China suggests that this is not just a sporadic act, but part of a well-planned strategy to gain economic, military, and political advantage. The points raised, such as involving the Chinese military or government employees, as well as involving Chinese nationals in most incidents, confirmed that there was coordination and support from the Chinese government in such espionage activities. This suggests that Chinese espionage is not an act carried out by an independent entity, but directed and supported by a higher power structure. China uses a variety of methods in its espionage activities, including traditional agency recruitment, unconventional approaches such as investment in property around military or research facilities, as well as cyber hacking. This shows China's flexibility and adaptability in exploiting loopholes in different security systems. China's focus on espionage has mainly centered on acquiring technology, both for military and commercial purposes. However, it is also important to note that such espionage also includes attempts to obtain information about U.S. civilian institutions or politicians, suggesting that China is interested in various aspects of U.S. life and policy. The complexity of Chinese espionage case agaist the U.S. can be seen from Table 1 below:

Table 1: The percentage of complexity of Chinese espionage case agaist the U.S.

Incidents directly involved Chinese military or government employees.	49%
Chinese citizens.	41%
Non-Chinese actors (usually Americans recruited by Chinese officials)	10%
Incidents involved cyber espionage, usually carried out by state-affiliated actors.	46%
Incidents attempted to obtain military technology.	29%
Incidents were attempts to obtain commercial technology.	54%
Incidents attempted to obtain information about US civilian agencies or politicians.	7%

Source: author's work

The downward trend in Chinese espionage after the agreement between President Obama and President Xi in 2015, was followed by a brief rescaling of events. The agreement aims to limit commercial espionage conducted by government entities, and improve relations between the U.S. and China when it comes to cybersecurity. However, the decline that followed the agreement was followed by a renewed increase in Chinese espionage activity within a year. This suggests that while the agreement may have created a period of relative peace in terms of commercial espionage between the U.S. and China, it has not been enough to significantly stop or completely reduce Chinese espionage activities. The brief decline was likely due to a temporary change in tactics or policy from the Chinese government, but the resurgence suggests that challenges in tackling Chinese espionage remain. Highlighting the complexities in efforts to control Chinese spying activities and the importance of continuing to push for strengthening agreements and cooperation in cyber security between the U.S. and China, as well as enhancing efforts in the detection, prevention, and countermeasures of cyber espionage at the national and international levels.

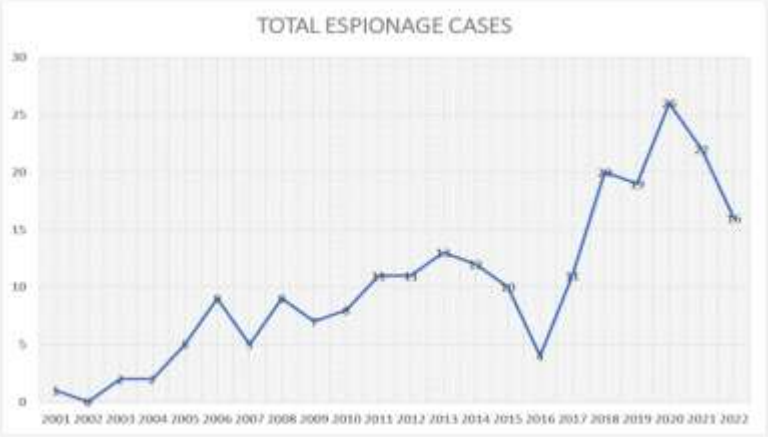

Figure 1: Number of espionage cases China conducts into the U.S. year over year

Source : CSIS

This data is taken from open source material and most likely does not reflect the full number of incidents. Most likely this is incomplete and more anecdotal than we would like. As with any list based on public information, the increase in the number of incidents could reflect increased activity after 2009 or could reflect increased public reporting on espionage cases, as greater attention is paid to the issue and the U.S. government becomes less reluctant (at the end of the Bush Administration) to publicly identify China as the culprit. Since this is only a reported case, and given the secretive nature of espionage, it most likely underestimates the true scope of the matter.

The involvement of Su Bin, a Chinese national who owns a factory in California in a cyber espionage case against the F-35 Joint Strike Fighter aircraft project, highlights the complexity and seriousness of the cyber espionage threat from rival countries such as China. In some cases, countries such as China may use their nationals who live or have businesses in the target country to conduct espionage activities.

In this case, the involvement of Chinese military officers to assist Su Bin in cyber espionage activities shows the coordination between civilian and military entities in efforts to steal sensitive information from other countries. Military involvement in cyber espionage activities is a serious concern as it shows that such countries are using their military resources to achieve espionage goals in the cyber domain.

Actions like these emphasize the importance of cooperation between law enforcement agencies, intelligence agencies, and the private sector in countering the threat of cyber espionage. Countries like the U.S. should increase their efforts in detecting, preventing, and responding to these kinds of cyberattacks by strengthening their cyber security, strengthening related laws and regulations, and enhancing international cooperation in combating cyber espionage.

Enhancing cyber security by the United States in solidarity with its NATO allies, including Estonia as the cyber hub of NATO members, is an important step in confronting modern cyber threats. Through NATO, member states are committed to helping each other and protecting each other from any threat, including cyber threats. Estonia has taken center stage in the context of cyber security due to their experience in dealing with significant cyber attacks in 2007. This incident is an important lesson for the international community about the importance of cyber security and cooperation in dealing with such threats.

The publication of President Obama's International Strategy for Cyberspace in 2011 reflected U.S. awareness of the importance of addressing cyber threats that could threaten national security and sovereignty. The strategy is designed to protect U.S. critical infrastructure, strengthen cyber defenses, and work with other nations to combat cyber threats globally. Measures like these show that countries like the U.S. recognize the importance of cyber security as a new domain in national and international security. Through cooperation in organizations such as NATO and policy strategies such as the International Strategy for Cyberspace, countries can jointly address cyber threats and build more resilient cyber security.

The improvement of cyber security by the United States (US) is indeed a natural response to the increasingly complex and serious threat of cyber attacks, including cyber espionage. Cyber espionage has become one of the most efficient and effective methods for other countries or entities to steal classified or sensitive information from other countries, including the defense industry.

The cyber espionage case you mentioned, conducted by the People's Republic of China against the U.S. military industry related to the F-35 Joint Strike Fighter military project, is a clear example of how countries use information technology to steal classified information of great value. The F-35 is a project of great importance to US national security, and information related to the project is of high strategic value.

The U.S. defense industry, like Lockheed Martin, is a prime target for cyberattacks because the information they possess can give a strategic advantage to competing nations. Therefore, the US must improve their cyber security not only in the military sector, but also in the private sector, including the defense industry, to protect their sensitive information from cyberattacks.

CONCLUSION AND RECOMMENDATION

From initially being considered an isolated threat, Chinese espionage has grown into a significant threat to the US. Perceptions of this threat have changed as China's large-scale espionage activities have increased, disrupting US foreign policy, trade and national security. China's espionage operations have expanded dramatically, increasing the number of operatives, personnel, government and state-owned companies, as well as foreign targets. The scale of China's espionage efforts has forced the US national security apparatus to adjust its policies, procedures and budgets. This reflects the need for adaptation in the way the US handles increasingly complex and ongoing espionage challenges. There is also a national construct (albeit excessive) to ensure intelligence information objectives are met by collecting foreign information and technology. The purpose of this information is related to national defense and economic priorities. This reflects China's strategy of using foreign information and technology to enhance its security and economic progress. The only important area in which China has shown little progress is its application of sophisticated trade espionage. China has a strong strategic interest in acquiring foreign information and technology, and they are prepared to face the risks and consequences that may arise from their operations. Lastly, China's espionage activities continue despite numerous arrests, public exposure, and most recently, US trade sanctions. One of the most significant impacts of Chinese espionage is on the US economy, primarily through intellectual property theft. Theft of technology, designs, and confidential business information can cause major losses to US companies and harm the country's economic competitiveness. Chinese espionage also threatens US national security by stealing sensitive military information, defense technology and critical infrastructure. This could strengthen China's capabilities in geopolitical competition and undermine US sovereignty and national security. China's espionage activities could impact U.S. political institutions and government by threatening integrity and trust in the political process. Additionally, it can influence political and policy decision-making, resulting in vulnerabilities in political and governmental systems. Thus, Chinese espionage has become a serious threat to US national security and economic interests. A comprehensive and effective response is needed to meet these challenges, including policy adjustments, increased law enforcement, international cooperation, and strengthening alliances. Only with a coordinated approach and multiple elements of national power involved can the US effectively address the threat of Chinese espionage.

REFERENCES

Buzan B. (1987) The Action-Reaction Model. In: An Introduction to Strategic Studies. International Institute for Strategic Studies Conference Papers. Palgrave Macmillan, London, https://link.springer.com/chapter/10.1007/978-1-349-18796-6_6 diakses 1 November 2017.

Cambia Research. (2016, 22 April). “Surface Web, Deep Web, Dark Web – What’s The Difference?”. https://www.cambiaresearch.com/articles/85/surface-web-deep-webdark-web----whats-the-difference

CNN Indonesia. (2016, February 22). "China's arms exports doubled" https://www.cnnindonesia.com/internasional/20160222114703- 113- 112511/China's arms-exports doubled/

Fajar Prasetyo, Ryan (2018) *South Korea's Cyber Security Policy After the Cyber Attack by North Korea (2009-2014).* Diploma thesis, Indonesian Computer University

Guntomo, Raharjo (2016) *United States Strategy in Facing China's Cyber Power Escalation for the 2011-2015 Period.* Bachelor thesis, Repository UIN Syarif Hidayatullah Jakarta

Jackson, Robert and Georg Sorensen, (2013), Elements of realism in Introduction to the Study of International Relations, Oxford University Press. p.112 Libicki, Martin. (1995). What is Information Cyberwarfare. National Defence Security

Llewellyn, J., & Thompson, S. (2020, September 22). Cold War Espionage. From Alpha History: https://alphahistory.com/coldwar/espionage/

McCarthy, Justin. 2016. "Americans Cite Cyber Terrorism among Three Major Threats to the US". *Gallup* , February 10. http://www.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx

McGraw, Gary. 2013. "Cyber Warfare Is Inevitable (Unless We Build Security)". *Journal of Strategic Studies* 36(1): 109–19.

Mulrine, Anna. 2016. "How North Korea is building a cadre of code fighters ready for cyber warfare". *Christian Science Monitor* , February 6. http://www.csmonitor.com/World/Passcode/2015/0206/How-North-Korea-built-up-a-cadre-of-code-warriors-prepared-for-cyberwar

Nazhif, N. J. (2022, September 27). Edward Snowden, US Secret Leaker Who Became a Russian Citizen. From https://context.id/read/630/edwardsnowden-pembocor-rahasia-as-yang-jadi-wn-rusia

New Media Institute. ”History Of the Internet”. http://www.newmedia.org/history-of-theinternet.html.

Nikolay Megits, D. M. (Vol.10 No.7 (2023*)). An economic analysis of the impact of the Russian War in Ukraine on the Poland-U.S. trade*. South Africa: JEECAR

Pratiwi, L. Y., &; Correia, Z. F. (2020). Cyber law: the practice of espionage in state sovereignty and diplomatic relations under the provisions of international law. Journal of Civic Education Undiksha Vol. 8 No. 3 , 1-13.

Devi, Purwanti (2019) Analysis of the United States' Motivation for Cybersecurity Cooperation with China. Diploma thesis, University of Andalas.

Reardon, Robert, and Nazli Choucri. 2012. "The Role of Cyberspace in International Relations: A Literary View". Paper presented at the 2012 ISA Annual Convention, San Diego, CA. April 1.

Ripsman, Norrin M., Jeffrey W. Taliaferro, and Steven E. Lobell. 2016. *Neoclassical Realist International Political Theory* . New York: Oxford University Press.

Rozak, A. (2020, December 29). Definition of Espionage, Characteristics, Causes, Impacts, and Examples. Retrieved February 7, 2023, from dosenppkn.com: https://dosenppkn.com/pengertian-spionase/

Service Care Solution. (Juni, 27 2016). ” Surface Web vs Deep Web vs Dark Web”.www.servicecare.org.uk-61792715468.

Get rid of it, Thomas. 2013. *Cyber War Won't Happen*. C Hurst &; Co. Publishers, Ltd.

Sindonews. (2017, October 14)." Form a cyber unit, the TNI is ready to face cyber attacks". https://nasional.sindonews.com/berita/1248299/14/bentuk-satuan-siber-tni-siap-hadapi-serangan-di-dunia-maya

Sterling, Bruce (1992). Hacker Crackdown Online and disorder on the electronic frontier: “Introduction”. http://www.gutenberg.org/files/101/101-h/101-h.htm

Valeriano, Brandon and Ryan C. Maness. 2015. *Cyber Warfare versus Cyberreality: Cyber Conflict in the International System*. New York: Oxford University Press.

Valeriano, Brandon and Ryan C. Maness. 2016. "Cyber Spillover Conflict: Transition from Cyber Conflict to Conventional Foreign Policy Dispute?". *Conflict in Cyberspace: Theoretical, Strategic, and Legal Perspectives,* ed. Jens Ringsmore and Karsten Friis, 45-64. London: Routledge.

Whyte, Chisthopher and B. Mazanec. 2019. *Understanding Cyber-Warfare.* New York: Routledge

Zetter, Kim. 2016. "Inside the cunning and unprecedented hacking of Ukraine's power grid". *Cable* . February 3. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

ABOUT THE AUTHORS

Ghina Arindiya, email: ghinarindiyaa@gmail.com

Ghina Arindiya is a student in the Department of international relations, Faculty of social and political sciences, Universitas Komputer Indonesia, Indonesia.

Dewi Triwahyuni, is is head of Department of International Relations at the Indonesian Computer University since 2018. Started her career as a lecturer since 2005. She obtained his Bachelor's, Master's and Doctoral degrees in the same field of International Relations. As a professional lecturer and has a Certified International Qualitative Researcher (CIQaR), Dr. Dewi Triwahyuni actively conducts research and writes scientific papers with a focus on International Relations, U.S. Foreign Policy and Cybersecurity.