International Journal of Research and Applied Technology

5(1)(2025) 82-92

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

Dynamics of The U.S.-China Relationship Post-Firewall Malware Attack

Dara Cantika Putriadin Boer*, **Fahriy Aulia Wardhana, Muhammad Arifin, Nadhira Fitria Zahra, Dewi Triwahyuni**
Universitas Komputer Indonesia, Indonesia

*Email: dewi.triwahyu@email.unikom.ac.id

Abstract. This study analyzes the impact of the Firewall Malware attack on US-China bilateral relations and its implications for global cybersecurity policy. The attack, detected in late 2024, exploited firewall vulnerabilities in US government and private sector systems, leading to significant data breaches. The US attributed the attack to a hacker group allegedly affiliated with the Chinese government, while China denied the allegations, escalating geopolitical tensions and undermining the 2015 US-China Cyber Agreement. Using a qualitative research methodology with a case study approach, this study examines government reports, cybersecurity analyses, policy statements, and media coverage, applying content analysis to assess geopolitical consequences and the effectiveness of international cybersecurity agreements. The findings reveal that the attack intensified US-China tensions, prompting sanctions, policy shifts, and heightened cybersecurity measures. The US reinforced its cyber defence strategies and imposed economic restrictions, while China sought to build alliances to counter the accusations. The study highlights the failure of existing international cybersecurity agreements in preventing state-sponsored cyber threats, emphasizing the urgent need for stronger global cooperation and regulatory frameworks to mitigate cyber conflicts and enhance cybersecurity resilience.

Keywords: China, Cyber Security, National Security, United States.

1. Introduction

Cyberattacks have become one of the biggest challenges for national and international security in recent years. One of the most striking phenomena is the cyberattacks carried out by state actors, especially those allegedly based in China, which have targeted critical infrastructure in various countries, including the United States. One recent case that attracted considerable attention was the arrest of a hacker suspected of being involved in developing and deploying malware that exploited thousands of systems worldwide. A report from the US Department of Justice also states that these attacks harm individuals and companies and threaten national security. This shows that cyber-attacks are not just a criminal act, but can also be a strategic tool in geopolitical competition between major countries.

In the process of making this research also examines several previous studies that are considered quite relevant to the topic being presented, namely cyber attacks, especially in the context of relations between the United States and China, including "China-US Cyber-attacks and International Security" written by Adenuga and abiodun (2023), "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence" [1]. SolarWinds Attack: Stages, Implications, and Mitigation Strategies in the Cyber Age" written by [2], 'China's Diplomacy towards the United States in CyberSpace 2015-2019' written by [3], "Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review" written by [4]. These studies include an analysis of China's cyberattacks, their impact on cyber security policies, and implications for the international relations of the two countries.

This research analyzes the dynamics of relations between the United States and China after the Firewall malware cyberattack. This research is quite different from some of the previous studies that have been mentioned, where in this study, the author emphasizes a more in-depth focus on the long-term impact of cyber attacks on the relationship between the two countries, foreign policy, and national security strategies of the two countries. This research is expected to contribute significantly to understanding how cyber attacks shape interactions between major countries in this digital era.

2. Literature Review

2.1. Cybersecurity Theory

The concept of security often goes beyond established political boundaries, framing certain issues as part of a specialized form of politics or even placing them outside the conventional political realm [5]. In the context of cybersecurity, securitization represents a heightened level of politicization, where digital threats are not merely seen as technical disruptions but also as strategic threats to national security and international relations [6]. According to Buzan (1998), there are three main approaches to understanding cybersecurity: Hyper Securitization, Everyday Security Practice, and Technotification [7]. Securitization occurs when a state takes drastic measures to protect its cyber domain, often involving technology experts to strengthen its digital defence systems [8]. Everyday Security Practice focuses on routine security measures implemented in daily life to minimize cyber risks, such as cybersecurity policies in both public and private sectors. Meanwhile, Technotification highlights the role of technology in enhancing security systems through continuous monitoring and rapid responses to evolving threats [9].

Cybersecurity itself encompasses various policies, strategies, and technologies designed to protect digital infrastructure from cyberattacks. In the context of U.S.-China relations following the Firewall Malware Attack, cybersecurity is not just a technical effort to prevent hacking but also a crucial aspect of their geopolitical rivalry. As demonstrated in this study, cyberattacks can significantly influence foreign policy, national security strategies, and the balance of power in the digital era.

2.2. Hybrid Warfare Theory

Hybrid warfare, as described by Igor Panarin, refers to a strategy where external actors manipulate protest-prone groups—often without their knowledge—and mobilize various disruptive forces, including extremist and criminal groups, to weaken an opposing regime. In today's digital age, hybrid warfare is no longer just about physical conflicts or propaganda;

cyber-attacks have become a powerful tool for disrupting economies, politics, and national security without engaging in direct military confrontation. This approach allows state and non-state actors to advance their strategic goals while avoiding international sanctions or diplomatic fallout [10].

In the case of U.S.-China relations, cyber-based hybrid warfare has increasingly shaped the dynamics between the two nations. The Firewall Malware Attack in late 2024 is a striking example, as it targeted critical U.S. infrastructure and heightened geopolitical tensions. The suspected involvement of hacker groups linked to the Chinese government only fueled further mistrust. Unlike traditional warfare, cyber-attacks operate in a grey zone−difficult to trace, easy to deny, and capable of causing significant disruption without triggering an outright military response. The nature of these attacks makes it challenging to assign blame definitively, as cyber operatives often hide their tracks using global proxy networks [10].

Beyond just cybersecurity, the political and economic repercussions of cyber-based hybrid warfare are far-reaching. The Firewall Malware Attack did not only damage networks; it reshaped diplomatic relations, influenced trade policies, and intensified the ongoing technological rivalry between the U.S. and China. In response, the United States imposed economic sanctions and reinforced cybersecurity measures, while China dismissed the accusations as politically motivated. As nations become increasingly dependent on digital infrastructure, cyber conflicts are expected to become a defining feature of modern geopolitics− where controlling cyberspace is just as critical as controlling land, sea, or air [10].

2.3. Balance of Power Concept

The concept of balance of power in international relations refers to strategies employed by states to maintain security and safeguard national interests by ensuring that no single power dominates absolutely. Wight outlines several interpretations of the balance of power, including the distribution of power among states, the principle of maintaining equilibrium within the international system, and the tendency of global politics to form power structures that prevent any one actor from gaining overwhelming dominance. In the realm of cybersecurity, the balance of power is not only about military strength but also about a country's ability to defend and counter cyber threats in the digital space [11].

The Firewall Malware Attack, detected in late 2024, exemplifies how the balance of power between the United States and China has evolved in cyberspace. The U.S. accused a hacker group allegedly affiliated with the Chinese government of orchestrating the attack, escalating tensions between the two nations. This incident highlights a key aspect of the balance of power theory, as the U.S. responded by reinforcing its cybersecurity capabilities and strengthening alliances with key partners to counter threats originating from China.

Additionally, the concept of alliances, as discussed by Walt, is relevant in understanding how states form strategic partnerships to enhance collective security against external threats. Walt emphasizes that alliances are driven by security concerns and are shaped by the evolving nature of threats. Following the firewall malware attack, the U.S. deepened its cooperation with allies such as the European Union, Australia, and Japan to develop a stronger cybersecurity strategy. This move demonstrates how alliances serve as a crucial mechanism in maintaining balance in geopolitical competition, particularly in the digital age [11].

Beyond military and political alliances, the balance of power in cybersecurity also involves the use of technology as a tool for diplomacy and deterrence. Cyberattacks are not merely about disabling a country's digital infrastructure; they also serve as strategic instruments in international competition. Both the U.S. and China have been engaged in a race to enhance their cyber capabilities, whether through technological advancements or stricter national security policies. The firewall malware attack, which targeted U.S. government agencies and private sector firms, underscores that the balance of power is no longer confined to traditional military domains but has expanded into the digital sphere [12].

In examining post-attack U.S.-China relations, the theories of balance of power and alliances offer valuable insights into how major powers respond to cyber threats. On one hand, the U.S. has sought to fortify its digital defences through regulatory measures and increased investment in cybersecurity. On the other, China has countered the allegations by shaping its narrative and expanding its influence in Asia and Africa through technological cooperation. Ultimately, this study illustrates that the firewall malware attack was not merely a technical security breach but a pivotal event with broader geopolitical implications. It reinforces the idea that balance of power and alliances remain central to international relations, particularly in navigating the challenges of cybersecurity in an increasingly digital world.

By understanding the existing data and some previous studies as well, we can gain a deeper insight into the dynamics that occur between the two countries after a cyberattack, specifically involving Firewall malware. Some of the previous studies used to help develop this research include:

(i) “China-US Cyber-attacks and International Security” (2023)
This journal discusses the tensions between China and the United States in the cyber world, where the two countries accuse each other of being the perpetrators of attacks. This research examines how cyber-attacks affect global security and emphasizes the importance of open dialogue to reduce tensions and build trust between the two countries.

(ii) “China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence” (2011)
This article discusses how China uses cyberattacks not only for espionage but also as a deterrence strategy. These attacks not only target infrastructure but also serve as political and military tools. The article also highlights the challenges countries face in protecting themselves from increasingly complex cyber threats.

(iii) “SolarWinds Attack: Stages, Implications, and Mitigation Strategies in the Cyber Age” (2024)
This journal reviews the SolarWinds attack, an example of a successful supply chain attack. It discusses how this attack occurred, its impact on various sectors, and mitigation strategies that can be implemented to protect critical infrastructure from similar attacks in the future.

(iv) “Cyber Security, Cyber Threats, Implications, and Future Perspectives: A Review” (2022)
This article discusses the various cyber threats that organizations face today, as well as the strategies used to protect information and infrastructure. The author emphasizes the need for a more holistic approach to cybersecurity management, including the integration of technology, processes, and people to address the evolving challenges in the digital world.

(v) “China's Diplomacy towards the United States on Cyberspace 2015-2019” (2022)
This research analyzes the diplomatic relations between China and the United States in the context of cyberspace from 2015 to 2019. It highlights how China, under the leadership of Xi Jinping, sought to promote policies of cyber sovereignty and cyber governance as part of its national strategy. China sees the United States as the dominant

power in cyberspace, making it important to conduct cyber diplomacy to reach mutual agreements and reduce tensions (Segal, 2017).

3. Method

Researchers used a qualitative approach with a descriptive-analytical type to analyze the dynamics of the relationship between the United States and China after the firewall malware cyber attack. The research data was obtained entirely from secondary sources, such as official government documents, news articles, academic journals, and related research. From the U.S. government, key sources include the 2023 DOD Cyber Strategy Summary (Department of Defense, 2023), the China-Based Hacker Charged in Cyberattack report (Department of Justice, 2024), and Treasury Department statements on sanctions against Chinese entities. Meanwhile, Chinese government sources include the National Cybersecurity Strategy (Cyberspace Administration of China, 2016) and official responses from the Ministry of Foreign Affairs (2024). The data collection technique was conducted through a literature study with thematic analysis to identify key issues in the context of cybersecurity and the dynamics of relations between the two countries. This research will conclude with key findings on the impact of cyberattacks on US-China bilateral relations.

4. Results and Discussion

A cyberattack known as the Firewall Malware Attack was first detected in late 2024 when several cybersecurity companies and United States government agencies discovered suspicious activity in firewall systems used by various important agencies. This malware is exploited through vulnerabilities in firewall devices that are widely used by government agencies and the private sector in the United States [13]. This attack has a very complex pattern, where hackers infiltrate firewall systems through the exploitation of zero-day vulnerabilities. Once inside, they deploy malicious code that enables system takeover and theft of sensitive data [14]. Some of the affected institutions include the US Treasury Department, major technology companies, as well as several research organizations that hold strategic information. The initial detection of this attack was made by BeyondTrust, a cybersecurity company that first reported anomalies in network activity. Further investigation revealed that this attack had been ongoing for several months before it was identified, indicating a highly organized level of planning and execution.

In an investigation conducted by US cybersecurity agencies, evidence was found that pointed to the involvement of a hacking group suspected of having affiliations with the Chinese government. A report from Kaspersky ICS CERT suggested that the attack patterns and code similarities matched those used by hacking groups such as APT 41 and Hafnium. It further reinforces the US perception that China is a major cyber threat. This view has long been part of the US security strategy, which assesses China's cyber activities as a form of influence expansion and a threat to national infrastructure. For the US, attacks like this are not just technical incidents, but also part of a broader geopolitical competition in the digital realm. As such, US cybersecurity policy has actively anticipated threats from China, as laid out in various official strategic documents.

However, attribution in cyberattacks is a highly complex process that often faces technical as well as political challenges. Many cybersecurity experts emphasize that attackers may deliberately leave false traces or utilize third-party infrastructure to obscure the origin of an attack. Therefore, while the US claims to have technical evidence such as attack patterns, code similarities, and IP addresses traced to China, the possibility of bias in these allegations needs to be considered [15]. Several pieces of evidence were found that point to the involvement of hacker groups allegedly affiliated with the Chinese government. The main evidence used to accuse China includes attack patterns that are consistent with methods used by hacking groups such as APT 41 and Hafnium, as noted in the Kaspersky ICS CERT report, code similarities with previous attacks launched by China-based groups, and targets attacked that indicate a geopolitical motive. In addition, some of the servers used in these attacks were traced to IP addresses based in China, despite attempts to disguise the traces by using global proxy networks. According to an official statement from the US Department of Justice and the Cybersecurity and Infrastructure Security Agency (CISA), this attack had links to state actors and was most likely supported by the Chinese government.

However, China itself strongly denied these allegations and accused the US of spreading propaganda without concrete evidence. In an official statement published by the Ministry of Foreign Affairs (MFA China) and reported by Global Times, Chinese Foreign Ministry spokesperson Mao Ning stated that such accusations were politically motivated and lacked solid evidence. China also stated that these accusations are designed to strengthen tensions between the two countries in the field of technology and digital security. Mao Ning also revealed that the US has been conducting large-scale and systemic cyberattacks against China for years. She emphasized the importance of the two countries working together to maintain cyber security, following the principles of equality, mutual respect, and abiding by international rules. Mao also called on the US to stop abusing sanctions in this context.

Following the Firewall Malware Attack and U.S. accusations, China strengthened its cybersecurity alliances and diplomatic efforts to counter international pressure. Beyond denying involvement, China pursued regional cybersecurity collaborations and digital sovereignty initiatives to enhance its cyber resilience. A key response was deepening cybersecurity cooperation with developing nations. In September 2024, during the China-Africa Cooperation Forum (FOCAC), China and African nations agreed to share cyber threat intelligence, develop digital surveillance technology, and prevent cybercrime. They also established joint incident response mechanisms and localized cybersecurity regulations aligned with China ’ s governance model. Similarly, in November 2024, through the Shanghai Cooperation Organization (SCO), China proposed a Cybersecurity Cooperation Framework, urging member states to coordinate cyber defence, limit foreign influence, and promote state-controlled internet policies, reinforcing its stance against Western cybersecurity dominance. Domestically, China expanded its Cybersecurity Law in December 2024, tightening data localization, counter-espionage measures, and restrictions on foreign tech firms. These measures align with the objectives of “China’s National Cyberspace Security Strategy, which prioritizes digital self-sufficiency and national security. By limiting foreign access to critical data and strengthening domestic technological capabilities, China aims to reduce reliance on external tech providers while countering cyber espionage threats. These policies reflect a broader strategy to fortify digital defences and assert cyber sovereignty. In response to the Firewall Malware Attack allegations, China has reinforced its cyber policies and expanded digital partnerships to safeguard its position in global cybersecurity governance.

Although China responded to these allegations with denial and highlighted the importance of cooperation in maintaining cybersecurity, tensions between the two countries over this issue have existed for years. One key moment in this ongoing tension occurred in 2015 when President Xi Jinping visited the United States to discuss cybersecurity issues with President Barack Obama. As a result of these discussions, the US-China Cyber Agreement 2015 was agreed upon. This agreement states that both countries agree not to commit cyber crimes such as cyber espionage, especially in the economic field. The 2015 US-China Cyber Agreement was originally designed to curb cyber economic espionage, but its enforcement declined as US-China tensions escalated due to the trade war and increasing technological rivalry. The agreement emphasizes the laws and measures that will be taken against cyber-attacks by both countries. This agreement is the first international agreement in the field of cybersecurity reached by two major countries, to avoid the use of cyber-attacks as a means of geopolitical competition. Initially, this agreement was considered quite effective in reducing hacking incidents between the two countries. Data from several cybersecurity agencies showed a decrease in economic espionage activities originating from China against US companies in the following years. However, the effectiveness of this agreement began to weaken after the increasing economic and political tensions between the US and China, especially after the trade war that began in 2018 under President Donald Trump. Along with increasing competition in the technology industry, especially in the fields of artificial intelligence and semiconductors, the two countries again suspected each other of covert cyberattacks.

The Firewall Malware attack demonstrated the inability of the 2015 US-China Cyber Agreement to prevent cyber activities that could escalate bilateral tensions. The increasing friction in recent years, mainly due to trade wars and technological rivalry, further undermined the agreement’s effectiveness and led both countries to accuse each other following the attack. The attack triggered a more aggressive US foreign policy response to China, including increased coordination with allies on cybersecurity and strengthening the national digital defence strategy. The United States also engaged its strategic alliances, including the Quad and NATO, to coordinate joint cybersecurity measures and counter China's growing cyber influence. In addition, the US accelerated the formulation of stricter regulations on technology companies with links to China, and increased cooperation with the European Union and its allies to build a more robust cyber defence system. On the other hand, China responded by strengthening its cyber sovereignty narrative and intensifying cyber diplomacy with developing countries, especially in Asia and Africa, to balance US dominance in global cybersecurity governance, which had previously been tense due to various issues, including trade wars, human rights, and conflicts in the South China Sea. The US government issued a strong statement condemning the hacking and demanding accountability from China. On the other hand, China retaliated by calling the US accusations an attempt to discredit their country on the international stage. After this incident, the United States tightened its cyber defence system by accelerating the implementation of stricter cybersecurity policies, including major investments in digital security technologies. This incident further strengthens US policies that seek to limit China's influence in the technology sector, including restrictions on cooperation with Chinese technology companies such as Huawei and TikTok. In addition, US allies such as the UK, Australia, and the European Union have also condemned this attack and supported US efforts to tighten cybersecurity regulations. Meanwhile, China is seeking to form alliances with other countries to rally support and reject the allegations.

In addition, a recent report from the US Treasury Department in January 2025 confirmed that this attack was categorized as a major incident under the Federal Information Security Modernization Act (FISMA). Further investigation indicated that the systems used for this attack originated from the exploitation of cloud services accessed by the US Treasury. In response to this attack, the United States took concrete steps to sanction the parties allegedly involved. These sanctions cover several aspects, among which are sanctions against individuals and hacker groups. The US Treasury Department announced a list of sanctioned individuals, including several Chinese nationals allegedly involved in the development and spread of the malware. The sanctions also target Sichuan Juxinhe Network Technology Co., LTD, a Sichuan-based cybersecurity company that the Treasury Department says was directly involved in a series of cyberattacks directed against major US telecommunications companies and internet service providers in the country.

The US government also imposed a ban on technology exports to several Chinese companies deemed to have links to these hacking activities. In addition, the US Department of Justice indicted several individuals suspected of involvement in these attacks and is seeking to work with allied countries to extradite the suspects. As a preventive measure, the US government is tightening regulations on companies that handle critical infrastructure to prevent similar attacks from happening in the future. These measures show that the United States is not only trying to respond to this attack technically but also using diplomatic and economic pressure to pressure China and warn other countries against similar actions.

Moreover, this incident confirms that the US-China rivalry in cybersecurity is not just a bilateral conflict, but also impacts broader global dynamics. According to the US Department of Defense Summary 2023, Since 2018, the US Department of Defense has been working with US allies to assist and identify vulnerabilities to networks operated by their governments. This operation conducted by USCYBERCOM has aided US cybersecurity preparedness. They have also helped improve the cyber resilience of their sector by exposing hostile TTPs and malware. On the other hand, China has responded by strengthening digital partnerships with developing countries in Asia and Africa, building an alternative narrative that US cyber dominance is a form of digital neo-hegemony that must be balanced. These tensions not only increase the risk of fragmentation in global internet governance but also accelerate countries' efforts to strengthen their digital autonomy to reduce dependence on cyberinfrastructure controlled by major powers.

With evidence suggesting the involvement of state actors, the US responded to this attack with strict sanctions as well as an upgrade of its cybersecurity system. This incident confirms that cyberattacks are not only a technological threat but also a geopolitical tool that can affect the dynamics of international relations in this digital age. Ultimately, the Firewall Malware Attack not only reflects the failure of the cybersecurity agreement once agreed between the US and China in 2015, but also sets a precedent for the escalation of digital conflicts in the future. This attack underlines that in the era of technology-based geopolitical competition, cyber is no longer just an instrument of defence, but a strategic arena in shaping the world order. The question is no longer whether countries will engage in cyber conflicts, but to what extent they can manage digital rivalries without triggering escalations that could potentially undermine global stability. Therefore, this incident should become a momentum for the international community to accelerate the establishment of more comprehensive global norms and regulations governing cybersecurity, to avoid the recurrence of incidents that could disrupt the world's geopolitical balance.

To better understand how this attack influenced US-China cyber relations and the global cybersecurity landscape, the following table presents a structured summary of key developments, including the attack’s detection, attribution to Chinese state actors, policy responses from both nations and its broader geopolitical implications.

Table 1. Key Developments in U.S.-China relations after the firewall malware attack

CATEGORY	KEY POINT	SOURCE
Detection of Firewall Malware Attack	Several U.S. government agencies and cybersecurity firms identified suspicious activities in firewall systems, affecting institutions like the U.S. Treasury Department and major tech companies.	**U.S. Department Of The Treasury** asury.gov/news/press-releases/jy2742#:~:text=WASHINGTON%20 –%20Today%2C%20the%20Department%20of,PRC **New York Post** https://nypost.com/2024/12/30/us-news/chinese-hackers-infiltrate-us-treasury-in-major-cyberattack-officials-tell-congress/
Attribution to Chinese State Actors	Investigations suggested involvement of Chinese-affiliated hacking groups, such as APT 41 and Hafnium, based on attack patterns and code similarities.	**Kapersky ICS CERT** https://ics-cert.kaspersky.com/publications/reports/2024/12/26/apt-and-financial-attackson-industrial-organizationsin-q3-2024/
China's Response	Chinese officials denied the allegations, accusing the U.S. of spreading unfounded propaganda without concrete evidence.	**Ministry of Foreign Affairs The People's Republic of China** https://www.mfa.gov.cn/eng/xw/fyrbt/lxjzh/202410/t20241014_11507287.html **Global Times** https://www.globaltimes.cn/page/202412/1324850.shtml
U.S. Sanctions and Defensive Measures	The U.S. imposed sanctions on individuals and entities linked to the attacks, including Sichuan Juxinhe Network Technology Co., LTD, and tightened cybersecurity regulations.	**U,S Departemnt Of The Treasury** https://home.treasury.gov/news/press-releases/jy2792 **Global Times** https://www.globaltimes.cn/page/202412/1324850.shtml
China's Cybersecurity Initiatives	China enhanced cybersecurity collaborations with developing nations and proposed frameworks through the Shanghai Cooperation Organization to promote state-controlled internet policies.	**The 2024 Summit of the Forum on China-Africa Cooperation** https://2024focacsummit.mfa.gov.cn/eng/zpfh_1/202409/t20240912_11489487.htm **The Shanghai Cooperation Organization** https://eng.sectsco.org/20180126/377347.html

CATEGORY	KEY POINT	SOURCE
Escalation of U.S.-China Cyber Tensions	The incident exacerbated existing tensions, leading to increased cybersecurity measures and strained diplomatic relations between the two nations.	**Ministry of Foreign Affais The People's Republic of China** https://www.mfa.gov.cn/eng/xw/fyrbt/lxjzh/202410/t20241014_11507287.html **Reuters** https://www.reuters.com/world/us/yellen-raised-serious-concern-about-chinas-malicious-cyber-activity-treasury-2025-01-07/

5. Conclusion

The Firewall Malware attack detected in late 2024 revealed a serious security vulnerability in the firewall infrastructure used by government agencies and the private sector in the United States. The exploitation of a zero-day vulnerability allowed hackers to infiltrate and take control of critical systems, indicating that cyberattacks today not only target data but also the integrity of security systems. Although technical evidence points to hacker groups affiliated with the Chinese government, attribution in cyberattacks remains complex and susceptible to bias. Evidence such as attack patterns, code similarities, and IP addresses linked to China must be carefully examined, considering the possibility of false traces and the misuse of third-party infrastructure. This incident not only impacts the technical domain but also has significant geopolitical implications. Governments worldwide, especially major powers, must strengthen dialogue and cooperation in the field of cybersecurity. Establishing multilateral agreements to regulate norms and rules in cyberspace will help prevent conflict escalation and promote global stability. The attack exacerbated tensions between the United States and China, disrupted cooperation in cybersecurity, and triggered the imposition of sanctions and stricter digital defence policies by the US. Government agencies and the private sector must conduct comprehensive evaluations and improvements to firewall systems and other security infrastructures. Investment in early detection technology and rapid response to zero-day exploitations should be a top priority.

References

[1] Adenuga, A. O., and Abiodun, T. E. (2023). China-US cyber-attacks and international security. *Nnamdi Azikiwe Journal of Political Science*, *8*(2), 86-97.

[2] Anisa, G., and Widianingsih, F. (2024). SolarWinds Attack: Stages, Implications, and Mitigation Strategies in the Cyber Age. *Electronic Integrated Computer Algorithm Journal*, *2*(1), 47-52.

[3] Birahayu, D. (2023). Maritime Digital Diplomacy: Legal Revitalization and Reform of Modern and Solutive Diplomacy. *Audito Comparative Law Journal (ACLJ)*, *4*(3), 170-184.

[4] Li, Y., and Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

[5] Sun, P., Doh, J., Rajwani, T., Werner, T., and Luo, X. R. (2024). The management of socio-political issues and environments: Toward a research agenda for corporate socio-political engagement. *Journal of Management Studies*, *61*(2), 277-306.

[6] Górka, M. (2023). Conceptualising securitisation in the field of cyber security policy. *Journal of Modern Science*, *53*(4), 263-290.

[7] Haryanto, A., and Sutra, S. M. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. *Global Political Studies Journal*, *7*(1), 56-69.

[8] Hansen, L., and Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175.

[9] Srijithesh, P. R., Gijo, E. V., Raja, P., Bhat, S., Mythirayee, S., Taallapalli, A. V. R., and Aravinda, H. R. (2025). Leveraging Lean Six Sigma principles in an Indian tertiary care hospital: a case study. *International Journal of Quality & Reliability Management*, *42*(2), 600-630.

[10] Prasetyawan, L. D., Maharanie, C., and Adilegowo, Y. (2023). Teknologi Intelijen dan Peperangan Hibrida. *Jurnal Kewarganegaraan*, *7*(2), 1942-1949.

[11] Khan, Z. F. (2025). Cyber Warfare and International Security: A New Geopolitical Frontier. *The Critical Review of Social Sciences Studies*, *3*(2), 513-527.

[12] Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and CounterIntelligence*, *26*(3), 453-481.

[13] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

[14] Ali, S., Rehman, S. U., Imran, A., Adeem, G., Iqbal, Z., & Kim, K. I. (2022). Comparative evaluation of ai-based techniques for zero-day attacks detection. *Electronics*, *11*(23), 3934.

[15] Mallick, M. A. I., and Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, *190*(1), 1-69.