The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 2, April 2025
https://doi.org/10.33022/ijcs.v14i2.4687

APT Winnti Panda as a Power-Gathering Tool in International Cyberspace

Rycka Septiasari[1], Yandry Kurniawan[2], Mohamad Arifandy[3], Erika Husna Nabila Putri[4]
rycka.septiasari@ui.ac.id[1], yandryk@ui.ac.id[2], mohamad.arifandy@ui.ac.id[3], erika.husna@bssn.go.id[4]
[1,2,3] Universitas Indonesia, [4]Badan Siber dan Sandi Negara

Article Information

Received : 3 Mar 2025
Revised : 7 Apr 2025
Accepted : 15 Apr 2025

Keywords

Advanced Persistent Threat, APT Winnti Panda, Cybersecurity, Cybersecurity Dilemma.

Abstract

This study provides an analysis of the Advanced Persistent Threat (APT) Winnti Panda impact on Indonesian infrastructure in 2022, which is a tool for gathering power in international cyberspace. The cybersecurity dilemma concept is utilized to explain the phenomena that occur using a deductive qualitative method. This study highlights how Indonesia perceives the cyber threats posed by the APT Winnti Panda. The data used in this study are primary data sourced from the Indonesian Cyber Security Agency (BSSN), which was taken through interviews. In addition, secondary data is also used using the archival and desk research methods from various online and offline sources. The main argument of this study is that the APT Winnti Panda, which attacked Indonesia in 2022, is a tool used to gather power in international cyberspace.

A. Introduction

The increasing global dependence on information technology in the digital era represents a crucial issue that must be addressed. Indonesia's technological infrastructure and internet network have experienced rapid development, which has opened opportunities for increasingly complex cyber threats. Indonesia's high cyberspace activity makes it a strategic target for cyberattacks. One type of cyber-attack that targets Indonesia is advanced persistent threat (APT). APT is a term used to sophisticated and organized cyberattacks, in which an attacker can remain in a target network for an extended period without being detected. APTs generally steal sensitive data or information, such as company secrets, customer data, and state intelligence information. APTs can also be operated by state-backed or non-state actors [1].

According to data from the Annual Report of the National Cyber and Crypto Agency (BSSN), in 2022, Indonesia experienced a 62% increase in APT attacks compared to 2021. In more detail, the three APT groups with the highest frequency of cyberattacks were the Ocean Lotus, Winnti, and Lazarus groups. Furthermore, compared to the previous year, some APTs have shown consistency and even an increase in attacks against Indonesia, particularly the APT Winnti Panda [2], [3]. APT Winnti Panda is a member of the Winnti Group, which is also known by other names, such as Blackfly and Wicked Panda. Based on reports from cybersecurity agencies, the proposed APT originated from China and has been operating since 2010 [4]. Initially, this group targeted the industrial sector. However, over time, APT expanded its operational targets to other sectors, including government agencies [5]. This APT group can steal various types of intellectual property, such as sensitive documents, blueprints, diagrams, formulas, and proprietary data related to manufacturing processes [6].

The stolen intellectual property data can be used to launch additional cyberattacks in the future. With the information they obtain, the group can exploit the victim network architecture, gain access to user credentials, steal employee emails, and collect customer data for subsequent attacks [6]. The Winnti Group continues to expand its data collection capacity. Information successfully obtained through attacks not only poses a significant threat to individual technological infrastructures but also jeopardizes the country's technological infrastructure and security.

The APT Winnti Panda attack, which originated from China and targeted Indonesia, is particularly noteworthy because the two countries have been engaged in cybersecurity cooperation since 2021. This cooperation is outlined in the Memorandum of Understanding (MoU) between the Cyberspace Administration of the People's Republic of China and the National Cyber and Crypto Agency of the Republic of Indonesia [7]. The agreement was signed on January 12, 2021, covering areas such as strengthening information exchange, sharing technology, enhancing cyber capacity, and collaborating to improve the data security ecosystem [7].

The cybersecurity cooperation between China and Indonesia is expected to serve as a framework for enhancing cybersecurity and technological capacity in both countries. Through the MoU, China and Indonesia have committed to upholding the principle of state sovereignty in cyberspace and to promoting a

democratic, transparent, and multilateral international internet governance system while ensuring data security. The agreement also emphasizes the development of a peaceful, secure, open, cooperative, responsible, and orderly cyberspace as well as the advancement of information and communication technology (ICT).

However, despite the agreement between the two countries, the situation has non been consistent with expectations. A year after the signing of the MoU, most cyberattacks on Indonesia's infrastructure originated from the APT Winnti Panda, a group linked to China. Given this background, this article aims to analyze the factors behind the increase in APT Winnti Panda's cyberattacks against Indonesia in 2022 despite the cybersecurity cooperation between the two governments.

B. Research Method

To conduct the analysis, this study refers to the concept of the cybersecurity dilemma proposed by Hersee [8] to understand the phenomenon of cyberattacks carried out by APT Winnti Panda against Indonesia in 2022 even though Indonesia had established a cybersecurity cooperation agreement with China a year earlier. The cybersecurity dilemma concept offers seven general characteristics that can explain the causes of cyberattacks from one party to another, namely: (1) anarchy in the international cyber system; (2) the need for cybersecurity among actors involved; (3) fear and uncertainty in the international cyberspace; (4) the inability to understand the other party's fears; (5) incompatible security; (6) efforts to gather power; and (7) efforts to increase insecurity and impose negative impacts on others. Among these seven characteristics, this study focuses on an analysis that seeks to explain cyberattacks as a means of consolidating power in an anarchic international cyberspace.

Furthermore, when operationalized in the context of this study, the research assumption is that APT Winnti Panda is a non-state actor capable of collecting intelligence information, which can then serve as a tool for gathering power in cyberspace. To analyze the empirical cases presented, this study applies a deductive qualitative approach [9]. This study aims to provide a detailed explanation of the process behind social phenomena and offer an in-depth understanding of the rise in cyberattacks of APT Winnti Pada against Indonesia in 2022, despite the cybersecurity cooperation agreement between Indonesia and China that had been established since 2021.

The data used in this study consisted of primary and secondary sources. The primary data were collected through interviews with representatives of the National Cyber and Crypto Agency (BSSN), which plays a direct role in ensuring cybersecurity in Indonesia. In addition, primary data were obtained from official government reports and international cybersecurity research institutions. The secondary data were derived from a literature review of various scientific journal articles, books, and news sources, both print and online. By combining primary and secondary sources, this study aims to obtain comprehensive and valid data to answer research questions. The data collection period covers 2021 to 2022, this timeframe was selected because Indonesia and China began implementing a cybersecurity cooperation agreement in 2021, and in 2022, APT Winnti Panda, which originated from China, carried out an unprecedented increase in

cyberattacks against Indonesia. The data obtained from interviews and literature reviews were then analyzed using narrative analysis, involving transcription and categorization to facilitate data processing. Then, the information was analyzed using variables aligned with the analytical framework. Based on this process, the findings were interpreted to answer the research questions regarding the cyberattacks conducted by APT Winnti Panda against Indonesia in 2022.

C. Result and Discussion

Advance Persistent Threat (APT) Winnti Panda or also known as APT41, BARIUM, and Blackfly, is a cyberattack group identified as a cyber threat group known to originate in China and has been operating since 2010. The Winnti Panda APT is a designation for a group of malicious software (malware) or malicious devices used by the state to conduct espionage [10]. Initially, the group targeted the gaming industry, starting with a fake antivirus product business in 2007. In 2009, they began targeting gaming companies in South Korea. However, over time, the group expanded the scope of attack targets to other sectors.

In its operations, the APT Winnti group uses malicious software (malware), which is a piece of software designed to damage, disrupt, or gain unauthorized access to a computer system or network. Malware is used by the Winnti Group to damage, disrupt, or gain unauthorized access to computer systems or networks and exfiltrate data from the systems it infiltrates. APT Winnti Panda disguises itself as an individual or a trusted organization to trick the target to conducting APT operations. Examples include communicating with victims (through phishing or spearphishing) by impersonating known senders such as executives, third-party providers, and colleagues. The trust formed from this disguise is then used to achieve the goals for many victims. In phishing cases that use business emails or email fraud, victims are tricked into sending money or leaking information that results in theft and financial losses.

The Winnti Panda APT also utilizes social engineering techniques, such as using manipulative and persuasive language in message headlines, such as payments, requests, or urging victims to take quick decisions before more severe incidents occur. These campaigns are often targeted at people who have roles that align with the targets of the opponent or attacker. APT Winnti Panda conducts identity impersonation, which usually begins with reconnaissance techniques such as collecting victim identity information and victim organization information as well as gaining access to infrastructure. such as email domains, to prove the false identity of the attacker. This capability has the potential to gain a large number of casualties in campaigns involving impersonation, for example, by breaking into an account targeting an organization that is then used to support the impersonation of other entities.

In addition to social engineering, APT Winnti Panda employs access token manipulation techniques. This technique allows attackers to exploit through authentication mechanisms, escalate access rights and perform lateral movements, or move gradually from one system to another within the same network. With access token manipulation techniques, attackers can behave as if they are the owners of the asset to gain access to the targeted resources [12]. This technique can be used to gather power in international cyberspace. The manipulated token

appears legitimate; thus, it is not detected by the security system. With access token manipulation capabilities, Winnti Panda's APT can achieve data theft, infrastructure infiltration, and espionage goals.

Then, Impersonation is another technique owned by APT Winnti Panda. With this code, attackers can impersonate a trusted person or organization to trick the target into conducting an attack. Attackers can communicate with victims in a phishing-like manner by impersonating a convincing-looking sender such as an executive, coworker, or third-party vendor [12]. Using the previously described tactics, techniques and procedures, the Winnti Panda APT can steal data, destroy documents, disrupt system performance, and spy on the activities of system or network users. In addition, the exfiltration technique conducted by APT Winnti Panda provides an overview of the strategic purpose behind the launched cyberattacks.

The capabilities of this cyber threat group that knows no national boundaries provide a very wide opportunity for it to transact with other parties, both with fellow non-state actors and with certain elements of state actors. This use is based on various backgrounds that motivate cyberattack operations. In general, APT group attacks have led to several motovations, including financial, political, ideological, selfishness, revenge, and espionage. Specifically, the Winnti Panda APT group tends to have a background of financial resources. This is reflected in the Winnti Group's APT, which has stolen thousands of gigabytes of intellectual property and sensitive proprietary data from various organizations across North America, Europe, and Asia. Such attacks cover the defense, energy, aerospace, biotechnology, and pharmaceutical sectors.

The ability of Winnti Panda has an impact that threatens the stability of other countries. which allows it to indirectly control the vital assets of the target country. The attack can be used as an opportunity to increase power in an anarchic international cyberspace. With the Winnti Panda APT, other actors, both fellow non-states and countries transacting with it, are able to gain access to the target system, thus supporting the collection of power in cyberspace using stolen or altered tokens, so that they can bypass existing security mechanisms and successfully enter other systems without being detected [12]. Based on the Techniques, Tactics, and Procedures (TTP) conducted by the Winnti Panda APT, it is known that from 2021 to 2022, this APT managed to compromise at least six US state government networks by exploiting web applications that are vulnerable to internet access.

Power is a complex concept that has various meanings that do not have a definite measurement mechanism. However, by definition, power refers to the capacity to achieve the desired or desired results, especially in influencing others. This definition varies based on user interests and values. Modern social science describes power through the "three faces of power" [13]. The first face, according to Robert Dahl (the 1950s), power as the ability to force others to act according to their preferences. The second face, according to Bachrach and Baratz (the 1960s) is power as the ability to set agendas, preventing problems from reaching the point of coercion. The third face, according to Steven Lukes (the 1970s), is the formation of beliefs and preferences that determine the desires of others. Power can also be

further divided into hard power (coercion) and soft power (persuasive), which reflect a spectrum from ruling behavior to cooperative behavior [13].

The Winnti Panda APT group can gain and increase power through its ability to influence other parties. Then the ability of the Winnti Panda APT group, which is able to steal data, destroy documents and disrupt system performance as well as spy on the activities of system and network users, is also able to gain power through this ability. Data security and intellectual property rights are particularly important for state and non-state actors. The information that is the target of the theft of the Winnti Panda APT is closely related to the country's economy, and even national security. Copyrights and trademarks are respected and enforced around the world because they are a form of state recognition for innovation and efforts made in research and development so that they deserve to be awarded.

On the other hand, there are some parties who believe that China is also a victim of various attacks from other countries. Therefore, the Winnti Panda APT operation, which is known to have originated from China, is also a defensive and offensive action by China. In addition, western countries are also taking advantage of this condition by glorifying China's cyberspace capabilities. This condition can be advantageous for certain countries to increase their national budgets [14]. The capabilities of Winnti Panda as an APT group are indeed possible to be used as a tool in efforts to gather power in cyberspace and can even cause cyber warfare. The use of cyberspace can pose the same dangers as conventional warfare because of the fundamental imbalance between attack and defense, as a result of technological complexity, and the costs required are not as high as those of conventional warfare [15].

Table 1. List of APT Groups originating from China.
Source: reprocessed from [1].

No	Identity	Active Time	Target Focus
1	1937CN	2016-2016	Critical infrastructure, cybercrime
2	APT10	2012-2022	Enterprises, critical infrastructure, cybercrime
3	APT31	2015-2018	Politics, cybercrime
4	APT40	2014-2019	Politics, companies, critical infrastructure, social groups, science, cybercrime.
5	APT41	2011-2023	Politics, corporations, critical infrastructure, science, cybercrime
6	Axiom	2009-2018	Politics, corporations, social groups, cybercrime
7	Emissary Panda	2010-2018	Politics, corporations, critical infrastructure, social groups, science, cybercrime
8	Honker Union	2001-2012	Politics, cybercrime
9	Ke3chang	2011-2022	Politics, corporations, critical infrastructure, cybercrime
10	Lotus Blossom	2017-2017	Politics, corporations, critical infrastructure, science, cybercrime,

11	MSS	2009-2018	Cyber infrastructure, cybercrime
12	MSS-supported Hackers	2014-2019	Critical infrastructure, cybercrime
13	Mofang	2012-2015	Politics, corporations, cybercrime
14	Mustang Panda	2021-2022	Politics, cybercrime
15	PLAN	2015-2018	Politics, corporations, critical infrastructure, cybercrime
16	Putter Panda	2007-2012	Politics, corporations, critical infrastructure, cybercrime
17	RedAlpha	2017-2018	Politics, corporations, social groups, cybercrime
18	RedEcho	2020-2021	Critical infrastructure, cybercrime
19	TA413	2021-2022	Social groups, cybercrime
20	Trip	2013-2018	Critical infrastructure, cybercrime

The Winnti Panda APT attack on Indonesian cyberspace conducted in 2022 is inversely proportional to the cooperation agreed upon by the two countries. In 2021, the Cyberspace Administration of China (CAC) of the People's Republic of China and the State Cyber and Cryptography Agency (BSSN) of the Republic of Indonesia conducted cybersecurity cooperation by signing a Memorandum of Understanding (MoU) on cybersecurity. This cooperation was agreed upon on January 12, 2021, with a scope that includes strengthening information exchange, technology sharing, increasing cybersecurity capacity, and collaborative efforts to strengthen the data security ecosystem. It is hoped that the cybersecurity cooperation between China and Indonesia will provide a foundation for developing cybersecurity and technology capacities in both countries. Through the ratified MoU, China and Indonesia are committed to respecting state sovereignty in cyberspace and encouraging the formation of an international internet governance system that is multilateral, democratic, transparent, and supports data security. The purpose of this collaboration is to create a peaceful, safe, open, cooperative, responsible, and orderly cyberspace, in line with the development of information and communication technology.

The Winnti APT attack can be categorized as a high-capability cyberattack supported by a country, with a specific purpose that intersects with political nuances. According to many cybersecurity reports, this attack originated in China and has the primary purpose of espionage against several countries. These attacks were actively detected since 2012 until the last report was published by Mandiant in 2024. An example is presented in the 2022 report, APT Winnti or also known as APT41, which conducted an attack targeting the computer network of the United States government. It was reported that the attack was successful and targeted as many as six computer networks of the United States government by taking advantage of vulnerabilities in the systems owned by the target of the attack using a series of attack techniques conducted. Furthermore, the last report submitted in 2024 showed that the APT41 attack successfully paralyzed several global organizations in the shipping and logistics, media and entertainment, technology, and automotive sectors. The targets of the attack are Europe, America, and Asia, including Italy, Spain, Taiwan, Thailand, Türkiye, and the United States. In this

action, which was reported in 2024, the perpetrator of the attack, known as Winnti Group, managed to gain unauthorized access to the internal network and obtain confidential data.

Furthermore, Winnti's APT attack also targeted Indonesia. The attacks were reported and detected from 2021 – 2024 [2], [3], [16], [17]. The distribution of APT Winnti attacks targeting Indonesia is shown.

Figure 1. Trend of Winnti APT Attacks in Indonesia

Based on this image, the peak number of attacks occurred in 2022 and remained active until 2024, although the number of attacks decreased. Some sectors or organizations affected by the Winnti APT attack included the government, the private sector, state-owned enterprises, banks, and telecommunications. However, it is possible that this attack activity attacks other sectors that have not yet been detected [2], [3], [16], [17]. These attacks employ complex methods to perform attacks, exploit vulnerabilities in a particular piece of software, infiltrate the network, and maintain access for an extended period of time. Some of the companies or applications that have been used to insert malicious programs as part of Winnti's APT attack campaign include Teamviewer, Gameforge, Marriot, and Lion Air.

Beyond the incident of the APT Winnti cyberattack that attacked Indonesia, there are interesting things that can be of concern. Indonesia and China have been cooperating with each other for a long time in various sectors. In 2023, led by President Joko Widodo [18], Indonesia established 10 Indonesia-People's Republic of China (PRC) bilateral cooperation. The cooperation covers the maritime, social, health, and economic sectors. Furthermore, at the end of 2024, President Prabowo and President XI agreed to strengthen their strategic partnership [19]. The agreement covers the fields of food, the economy, and resources. Cooperation in the cybersecurity sector was also conducted in 2021 between Indonesia and China through the State Cyber and Cryptography Agency of the Republic of Indonesia and the Cyberspace Administration of the People's Republic of China, namely cooperation in cybersecurity and technology capacity building [20]. The

cooperation has an action plan that includes the following: 1) Encouraging the exchange of information on regulatory systems related to cyberspace governance. 2) Sharing views, experiences, lessons learned, and best practices on the protection of vital information infrastructure, cyber threat mitigation, and cooperation from each Party. 3) Conduct and facilitate dialog on cybersecurity issues between the government, institutions, academics, commercial industry, and other relevant stakeholders, as well as encouraging mutual trust and cooperation in the field of data security. 4) Encouraging and coordinating the visit of cybersecurity experts between Indonesia and China. 5) Facilitating exchanges and training programs on cyberspace defense technologies and methods among relevant stakeholders. 6) Encouraging cooperation in capacity building on cybersecurity issues related to the protection of vital information infrastructure, data security management, protection of personal information, and cyber threat countermeasures [21].

The many collaborations conducted by Indonesia and China invite certain parties to get an advantage. Moreover, cooperation not only benefits Indonesia in terms of infrastructure improvement and development, but also benefits China because Indonesia is considered a major contributor to business carried out by China [22]. This is supported by the occurrence of APT Winnti's highest attack attempt on Indonesia in 2022, or a year after cybersecurity cooperation between Indonesia and China occurred. Sectors detected to be affected by Indonesia can also be an illustration that the sector is a strategic sector owned by Indonesia. The actions of APT Winnti in Indonesia can be a tool for capitalizing or the accumulating power over Indonesia.

To respond to this threat, the BSSN, which is a cybersecurity institution operating on a national scale in Indonesia, took several steps in response to detected attacks. BSSN validates the attack launched by the Winnti Panda APT group and attempts to identify the party or entity behind the attack. This step is important for understanding how the motives, affiliations, and support from certain countries, organizations, or groups behind the attacks occurred. In this organized APT attribution or attacker tracking process, an in-depth analysis involving six main aspects is performed, as described in the Attribution of Advanced Persistent Threat. These six aspects are often summarized as MICTIC and include malware, infrastructure, control server, telemetry , intelligence , and Cui Bono. Each aspect provides clues for cyber analysts to identify the perpetrators or funders of the attacks.

A thorough analysis of the six aspects of MICTIC, BSSN, and other cyber institutions can provide a clearer picture of the Winnti Panda APT. This kind of investigation helps not only identify the perpetrators of the attack but also in formulate future cyber threat mitigation strategies. Despites cyberattacks, the BSSN, through the Directorate of Cybersecurity Operations, performs the identification, protection, detection, response, and recovery. These five functions are intertwined to minimize the risk of cyberattacks and are aligned with the NIST Cybersecurity Framework (CSF). The NIST Cybersecurity Framework (CSF) is a guide designed to assist organizations in managing and mitigating cybersecurity risks.

The efforts made by Indonesia are defensive by implementing certain measures and not taking offensive steps. In addition, Indonesia actively participates in capacity building and sharing information related to the latest cyber threats with other countries. Indonesia also strengthens cybersecurity cooperation relationships with both states and non-state organizations and improves cybersecurity at the national level, including in central and regional institutions, to address the latest cyber threats. Indonesia is also striving to increase the cybersecurity awareness of the Indonesians so they can be more vigilant about APT activities. Some of the programs carried out include routinely issuing warnings and advisories regarding cyber threats, including threats from APT Winnti Panda; actively conducting cybersecurity training and literacy for various parties; improving national cybersecurity infrastructure; and actively participating in various international forums to share information about the latest cyber threats and adopt best practices in cybersecurity.

D. Conclusion

This study applies a variable from Hersee's cybersecurity dilemma theory [8], namely the tendency of actors to accumulate power. This characteristic is then operationalized into variables used to analyze the phenomenon under investigation. The focus of this study was on the efforts of APT Winnti Panda. Based on the analysis conducted, APT Winnti Panda is a non-state group capable of exploiting the anarchic nature of international cyberspace to strengthen its cyber capabilities and gain strategic leverage when interacting with other actors with competing interests in cyberspace. The APT Winnti Panda has been found to collect intelligence from multiple sectors across various countries, including Indonesia.

Through its techniques, tactics, and procedures, the cyberattacks launched by APT Winnti Panda against Indonesia in 2022 posed a significant cybersecurity threat. These attacks employed sophisticated methods aimed at stealing the country's strategic information. The occurrence of these attacks despite cybersecurity cooperation between Indonesia and China highlights the presence of a cybersecurity dilemma. In response to these attacks, Indonesia has focused on conducting technical analyses to enhance its cybersecurity parameters without engaging in retaliatory actions against the attacking country. This study also argues that the concept of the cybersecurity dilemma is sufficiently relevant in explaining the cyberspace conflict between Indonesia and China in 2022. However, this concept has limitations. The increasing complexity and dynamic nature of cyberspace pose challenges in fully explaining cyberconflicts through the cybersecurity dilemma framework because it is an adaptation of the traditional security dilemma concept. Research on the cyberspace security dynamics between Indonesia and China should not be stopped. This study can pave the way for future research that can uncover alternative perspectives on cybersecurity relations between China and Indonesia.

E. References

[1] MITRE ATT&CK, “APT41.” Accessed: Feb. 01, 2025. [Online]. Available: https://attack.mitre.org/groups/G0096/

[2] Badan Siber dan Sandi Negara, "Laporan Tahunan Monitoring Keamanan Siber 2021," 2021.
[3] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2022," 2022.
[4] Mike Stokkel *et al.*, "APT41 Has Arisen From the DUST," Google Threat Intelligence Group. Accessed: Feb. 01, 2025. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust
[5] MITRE ATT&CK, "Winnti Group." Accessed: Oct. 30, 2024. [Online]. Available: https://attack.mitre.org/groups/G0044/
[6] T. H. News, "Chinese Hackers Caught Stealing Intellectual Property from Multinational Companies," 2022. Accessed: Nov. 26, 2023. [Online]. Available: https://thehackernews.com/2022/05/chinese-hackers-caught-stealing.html
[7] Kementerian Luar Negeri RI, "Memorandum of Understanding between the National Cyber and Crypto Agency of the Republic of Indonesia and the Cyberspace Administration of the People's Republic of China on Cooperation in Developing Cyber Security Capacity and Technology." Accessed: Nov. 26, 2023. [Online]. Available: https://treaty.kemlu.go.id/apisearch/pdf?filename=CHN-2021-0228.pdf
[8] S. Hersee, "The Cyber Security Dilemma and The Securitisation of Cyberspace," University of London, 2019.
[9] W. L. Neuman, *Social Research Methods: Qualitative and Quantitative Approaches*, 7th ed. Harlow: Pearson Education Limited, 2014.
[10] WeLiveSecurity, "Menghubungkan titik-titik: Mengungkap persenjataan dan metode Grup Winnti." Accessed: Oct. 31, 2024. [Online]. Available: https://www.welivesecurity.com/2019/10/14/connecting-dots-exposing-arsenal-methods-winnti/
[11] ETDA, "APT group: Winnti Group, Wicked Panda." Accessed: Oct. 30, 2024. [Online]. Available: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Winnti Group%2C Wicked Panda. Lihat juga, QuoIntelligence, "WINNTI GROUP: Insights From the Past." Accessed: Oct. 30, 2024. [Online]. Available: https://quointelligence.eu/2020/04/winnti-group-insights-from-the-past/.
[12] MITRE ATT&CK, "Access Token Manipulation." [Online]. Available: https://attack.mitre.org/techniques/T1134/
[13] J. S. Nye, "Cyber Power," 2010.
[14] M. Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *J. Strateg. Secur.*, vol. 4, no. 2, pp. 1–24, 2011.
[15] G. Kartasasmita and A. P. Kurnadi, "The Securitization of China's Technology Companies in the United States of America," *J. Ilm. Hub. Int.*, vol. 16, no. 2, pp. 159–178, 2020, doi: 10.26593/jihi.v16i2.4204.159-178.
[16] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2023," 2023.
[17] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2024," 2024.
[18] Kementerian Luar Negeri, RI "Presiden Jokowi dan Presiden Xi Jinping Bahas Kerja Sama Bilateral Indonesia-RRT." Accessed: Feb. 01, 2025. [Online].

Available: https://kemlu.go.id/berita/presiden-jokowi-dan-presiden-xi-jinping-bahas-kerja-sama-bilateral-indonesia-rrt?type=publication
[19] Kementerian Luar Negeri RI, "Presiden Prabowo dan Presiden Xi Sepakat Perkuat Kemitraan Strategis Indonesia-Tiongkok." Accessed: Feb. 01, 2025. [Online]. Available: https://kemlu.go.id/berita/presiden-prabowo-dan-presiden-xi-sepakat-perkuat-kemitraan-strategis-indonesia-tiongkok?type=publication
[20] H. Alaydrus, "Luhut Teken MoU Pengembangan Internet dengan China. Indonesia Pakai 5G Huawei?" Accessed: Feb. 01, 2025. [Online]. Available: https://ekonomi.bisnis.com/read/20210124/9/1346985/luhut-teken-mou-pengembangan-internet-dengan-china-indonesia-pakai-5g-huawei
[21] Kementerian Luar Negeri RI. "Rencana Aksi 2022-2024 Sebagai Implementasi Memorandum Saling Pengertian Antara Badan Siber dan Sandi Negara Republik Indonesia Dan Administrasi Ruang Siber Republik Rakyat Tiongkok Tentang Kerja Sama Pengembangan Kapasitas Keamanan Siber dan Teknologi," Jakarta & Beijing, 2022.
[22] A. R. Arianto, D. Maarif, Muhadjir, and R. Argaditya, "Indonesia-China Cooperation For The Development And Improvement of Digital Technology 4.0 in The Field of Security And Economy," *Glob. Komun.*, vol. 5, no. 2, pp. 42–51, 2022.