International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 49 No. 1 February 2025, pp. 663-672

# *Exploration of Tactics, Techniques, and Procedures (TTP) in Cyber Attacks on Government Infrastructure*

Firman Faidin, H.A Danang Rimbawa, J. W. Saputro[1]

Master of Cyber Defense Engineering, Faculty of Defense Science and Technology

The Republic of Indonesia Defense University

Bogor, Indonesia[1]

firman.faidin@tp.idu.ac.id



**Abstract— Cybersecurity has become a crucial issue in protecting government infrastructure in the digital era. Cyberattacks are increasingly sophisticated and structured using a variety of evolving Tactics, Techniques, and Procedures (TTPs). This research aims to explore the patterns of cyberattacks targeting government systems and understand how TTPs are used by threat actors to penetrate, exploit, and disrupt critical infrastructure. The research method used is qualitative with a case study approach and in-depth interviews with cybersecurity experts, threat analysts, and relevant officials in the government sector. In addition, this research also reviewed documented cyber incident reports to identify frequent attack patterns. The results show that cyberattacks against government infrastructure are generally carried out through spear-phishing, exploitation of software vulnerabilities, and persistence techniques to maintain illegal access. In addition, threat actors often use lateral movement methods to spread attacks to wider systems. The study also found that most attacks capitalize on gaps in security policies and lack of employee awareness as key success factors. In conclusion, an in-depth understanding of the TTPs used in cyberattacks can help improve mitigation strategies, strengthen security policies, and develop early detection systems to protect government infrastructure from increasingly complex threats.**

**Keywords— cybersecurity, cyberattacks, technical tactics and procedures (TTP), government infrastructure, cyber threats.**

## I. INTRODUCTION

Cybersecurity has become one of the strategic issues in the digital era, especially for the government sector that manages sensitive data and critical infrastructure (Djenna et al., 2021). Cyberattacks targeting government infrastructure can have far-reaching impacts, ranging from data leakage, disruption of public services, to threats to state sovereignty (Dawson et al., 2021). In Indonesia, the increasing incidence of cyberattacks against government institutions indicates an urgent need to understand the attack patterns and methods used by threat actors (Edy et al., 2017). In the world of cybersecurity, the concept of Tactics, Techniques, and Procedures (TTP) is often used to analyze how cyberattacks are carried out. TTP is an approach that helps in identifying the strategies and methods used by threat actors to exploit target systems. Tactics reflect the goal the perpetrator is trying to achieve, techniques explain how a tactic is implemented, while procedures refer to the specific steps taken to execute an attack (Bahrami et al., 2019).

Exploration of the TTP is crucial in efforts to improve government cyber resilience. By understanding how attacks are carried out, defense systems can be developed more effectively to detect, prevent and respond to threats quickly. Therefore, this research focuses on an in-depth analysis of TTPs used in cyberattacks against government infrastructure. Cyberattacks targeting government

systems often use a variety of complex and diverse methods. Some common methods used include spear-phishing, software vulnerability exploitation, social engineering, and malware attacks (Diogenes et al., 2019). Spear-phishing, for example, is one of the most used techniques as it takes advantage of government employees' inattentiveness in accessing malicious links or attachments. In addition, software vulnerability exploitation is also a technique often used by attackers. Vulnerabilities in systems that are not updated or have flaws in the code can be exploited to gain unauthorized access to government systems. These attacks are often carried out using the zero-day exploit method, where the perpetrator takes advantage of weaknesses that have not yet been identified by the software developer. Another technique often used in cyberattacks is lateral movement, which is an attacker's attempt to move from one system to another after successfully gaining initial access (Aslan et al., 2023). This technique allows the attack to spread more widely within the government network, increasing the scale of the impact of the attack.

Cyberattacks against government infrastructure also often involve persistence mechanisms, which are techniques used to maintain access to systems for extended periods of time. Threat actors may install backdoors or hard-to-detect malware to ensure that they can continue to access target systems despite recovery or repair efforts. The main factors contributing to the success of cyberattacks against governments are gaps in cybersecurity policies and lack of employee awareness of cyber threats (Baker, B., 2019). Many government organizations still have security policies that are not well standardized or do not implement strict preventive measures. In addition, the lack of cybersecurity training for employees increases the risk of successful social engineering-based attacks (Andress et al., 2013).

In recent years, Indonesia has experienced numerous cyberattacks targeting government agencies, including sensitive data leaks, official website defaces, as well as ransomware attacks that resulted in the paralysis of digital services. These attacks show that threat actors continue to develop new methods to exploit weaknesses in government cyber defense systems. As a mitigation effort, the government has developed various policies and regulations related to cybersecurity, such as the establishment of the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara or BSSN) and the implementation of information security policies based on international standards. However, challenges remain in the implementation of these policies, especially in terms of inter-agency coordination, resource allocation, and improving the capabilities of experts in the field of cybersecurity (Yulianto, A., 2021).

This research uses a qualitative method with a case study approach and in-depth interviews to understand how TTP is applied in cyberattacks against government infrastructure. Data was obtained from various sources, including cybersecurity incident reports, interviews with cybersecurity experts, and analysis of documented attack patterns (Yaseen, A., 2020). The results of this research are expected to provide greater insight into the strategies used by threat actors in targeting government infrastructure. With a better understanding of TTP, government agencies can design more effective defense measures to improve national cyber resilience. Thus, this research not only contributes to an improved understanding of the dynamics of cyber attacks, but also serves as a basis for the development of more adaptive and resilient cybersecurity policies in the face of future digital threats.

## II. Literature Review

### *A. Tactics, Techniques, and Procedures (TTP)*

In the realm of cybersecurity, the concept of Tactics, Techniques, and Procedures (TTP) serves as a basic framework for understanding the workings and operational strategies employed by threat actors. Tactics describe the strategic goals of an attack, techniques describe the methods applied to achieve those goals, and procedures describe the specific operational steps performed during an attack. An in-depth understanding of the TTP enables early identification and proactive countermeasures against threats as it provides a comprehensive picture of the attacker's modus operandi (Yaseen, A., 2020). Frameworks such as the Cyber Kill Chain, uses TTP to map the stages of an attack from reconnaissance to data exfiltration. This approach helps security researchers and practitioners find critical points where interventions can be made to prevent or mitigate the impact of attacks and enables the design of defense strategies that are more adaptive to the evolution of attack techniques (Diogenes et al., 2019).

Recent research has shown that Advanced Persistent Threat (APT) groups often utilize complex TTPs to penetrate security systems (Sfetcu, N., 2024). For example, APT29 groups use spear phishing as a tactic to gain initial access, then apply lateral movement techniques to extend penetration into internal networks, thus obscuring the attack trail and demanding improved detection

and response capabilities from defense systems (Bahrami et al., 2019). While many studies have examined TTP in the context of cyberattacks, there is a lack of literature that specifically addresses the application of TTP to government infrastructure. Most studies still focus on the private sector or attacks in general without considering the unique dynamics and vulnerabilities of government systems. Therefore, further exploration of the application of TTP in the context of government is needed to fill the research gap and strengthen cyber defense strategies in this sector (Yaseen, A., 2020).

### *B. Cyber Attacks*

Cyberattacks are structured attempts to access, damage, or disrupt information systems through digital networks. Various types of attacks, such as malware, phishing, denial-of-service (DoS), and ransomware, have emerged and shown an increase in frequency and complexity, posing a major challenge to system protection, especially in the government sector (Lee, N., 2024). As technology advances, attackers are increasingly adopting advanced techniques, such as zero-day exploits and fileless malware, which can evade traditional detection systems. In addition, social engineering-based attacks-especially spear phishing-utilize human weaknesses in the identity verification process, confirming that cyberattacks are not solely technical, but also involve psychological strategies to exploit target vulnerabilities.

The impact of cyberattacks on government systems is significant, as the attack methods used often result in sensitive data leaks and disruptions to public services. This suggests that attackers are strategically adjusting their methods to exploit gaps in government infrastructure, requiring a more integrated and responsive approach to defense (Yaseen, A., 2020). Recent trends show that cyberattacks are increasingly relying on artificial intelligence and machine learning to optimize attack tactics in real-time. In addition, the increasing interconnection of digital systems and the utilization of Internet of Things (IoT) technologies open new opportunities for attackers to conduct large-scale attacks. Therefore, an in-depth understanding of the evolution of cyberattack techniques is critical to developing mitigation strategies that are adaptive to changing threat dynamics (Lee, N., 2024).

### *C. Government Infrastructure*

Government infrastructure includes all facilities, systems, and networks that support state administration operations (ranging from data centers, e-government systems, to internal communication networks) which are the backbone of public service providers and strategic information management (Larasati et al., 2016). During increasing digitalization, the need for stronger protection against cyberattacks has become urgent. On the other hand, government infrastructure vulnerabilities often arise due to the use of outdated systems, suboptimal security configurations, and a shortage of cyber experts. These gaps are often exploited by attackers to infiltrate networks and access sensitive data. These challenges are further compounded by budget constraints and a lack of consistent security standards across agencies, increasing the risk of far-reaching cyberattacks (Clarke, 2019).

In response to these threats, the government has implemented various strategies to strengthen its security system. These include improving monitoring systems, implementing advanced encryption technologies and regular training for employees. While these measures have had a positive impact, an in-depth evaluation of the implementation of Tactics, Techniques and Procedures (TTP) in cyberattacks is still needed to identify specific gaps and develop more effective policies in maintaining the integrity of government infrastructure (Ramadhianto et al., 2024).

### *D. National Security*

National security in the digital age involves protecting not only the physical territory, but also the integrity of information systems that support government operations and public services. Cyberattacks on critical infrastructure can disrupt political, economic and social stability, so cyber resilience should be a national priority through collaboration between the public sector, private sector and international institutions (Ramadhianto et al., 2024). In addition, large-scale attacks have the potential to undermine public trust, disrupt vital services and threaten the democratic process through the manipulation of election data, which has a strategic impact on the overall stability of the country (Clarke, 2019). To counter these threats, developed countries have developed national cyber defense strategies by establishing specialized units and adopting frameworks such as the National Cybersecurity Strategy. In Indonesia, the government through BSSN has formulated a National Cybersecurity Strategy that emphasizes the integration of advanced technologies, increased human resource capacity, and inter-agency collaboration to

strengthen defenses (Scarfone et al., 2007; Ramadhianto et al., 2024). Despite these efforts, challenges such as technological limitations, shortages of experts, and inter-agency coordination remain significant obstacles, necessitating international cooperation, investment in technology, and increased training. An in-depth understanding of Tactics, Techniques and Procedures (TTP) in cyberattacks is expected to be an important foundation in formulating effective mitigation strategies to protect government infrastructure and strengthen national security in the digital era.

## III. Research Methods

This research uses a qualitative approach with descriptive methods to explore in depth the Tactics, Techniques, and Procedures (TTP) in cyber attacks on government infrastructure. The descriptive method allows researchers to obtain a detailed description of the phenomenon under study through contextual and comprehensive data collection. Data were collected through in-depth interviews with cybersecurity experts, government officials, and incident analysts, as well as through documentation studies and participatory observation of cyber incident reports and related publications (Creswell et al., 2023). Furthermore, data analysis was conducted using thematic analysis methods to identify patterns, relationships and dynamics between TTPs used by threat actors and their impact on government infrastructure (Baker, B., 2019).

This descriptive approach was chosen because it provides a holistic understanding of how cyberattacks and attackers' operational strategies work and allows for the depiction of challenges and opportunities in strengthening cyber defense systems in the government sector. In addition, a data triangulation strategy was used to increase the validity of the findings through comparison between different data sources and collection techniques, resulting in a more in-depth and comprehensive analysis (Creswell, 2021). Thus, this research is expected to make a significant contribution to the formulation of appropriate mitigation strategies to protect government infrastructure from increasingly complex cyber threats.

## IV. Discussion

The discussion also emphasized the importance of cross-agency collaboration and integration of advanced technologies to formulate effective mitigation strategies. With an in-depth understanding of the TTP, policy recommendations can be developed to improve preparedness for evolving cyber threats, making government infrastructure security efforts more resilient and responsive to the dynamics of digital attacks.

### *A. Reconnaissance*

Reconnaissance is the initial stage in a cyber attack where the attacker gathers as much information as possible about the intended target. The main goal of this stage is to understand the structure, weaknesses, and potential security holes that can be exploited in subsequent stages of the attack. Effective reconnaissance allows attackers to plan attacks with more precision and increase the chances of success (Khan et al., 2018). There are two main types of reconnaissance: passive and active reconnaissance. Passive reconnaissance is performed without direct interaction with the target system, thus reducing the risk of being detected. Techniques used in this method include OSINT (Open Source Intelligence), which is the collection of data from open sources such as official websites, social media, public forums, and online databases, which can provide information about an organization's structure, technology used, and security policies implemented (Evangelista et al., 2021). In addition, there is also dumpster diving, which is the search for sensitive information discarded by the organization, such as physical documents, records, or hardware that is no longer in use.

Meanwhile, active reconnaissance involves direct interaction with the target system to identify specific weaknesses, although it is riskier because it can be detected. Some of the techniques used include scanning, which is scanning the network to find open ports, running services, and potential vulnerabilities using tools such as Nmap (Chauhan, 2018). Another technique is social engineering, where the attacker manipulates individuals within the target organization to reveal sensitive information, such as through phishing. There is also footprinting, which is a systematic process of identifying and collecting information about the target's network, operating system, and system architecture, including IP addresses, server details, and network configuration.

*B. Weaponization*

Weaponization is the second stage in the cyber attack chain known as the Cyber Kill Chain. In this phase, the attacker utilizes the information gathered during the reconnaissance phase to develop or modify specific attack tools, such as malware or exploits, designed to exploit vulnerabilities found in the target. The main objective of this stage is to prepare an effective cyber weapon for use in the next stage of the attack (Khan et al., 2018). In the context of government infrastructure, the weaponization stage plays a crucial role. These infrastructures often rely on complex systems and networks, which, if successfully compromised, can have a significant impact on national security and public services. Therefore, attackers typically invest considerable time and resources to ensure that their attack tools can penetrate existing defenses. Common techniques used in this stage include the development of custom malware, utilization of zero-day vulnerabilities, creation of malicious documents, and development of exploits for SCADA (Supervisory Control and Data Acquisition) systems that are often used in critical infrastructure such as power plants or transportation systems (Pliatsios et al., 2020). To protect government infrastructure from threats at the weaponization stage, several mitigation measures can be implemented. Regular system updates and patches are essential to close security gaps that can be exploited by attackers. Implementation of intrusion detection and prevention systems (IDPS) can help in detecting suspicious activity before an attack occurs (Scarfone et al., 2007). Additionally, security awareness training for employees is necessary so that they can recognize tactics such as phishing that are often used to spread malware. Finally, collaboration between agencies and the private sector is essential to share information on the latest threats and effective defense strategies.

*C. Delivery*

Delivery is the third stage in the cyber attack chain known as the Cyber Kill Chain. In this phase, the attacker delivers an attack tool, such as malware or an exploit, to the target system with the goal of gaining initial access. The success of this stage depends largely on the delivery method used and how well the attacker can trick the target into accepting and executing the attack tool (Tarnowski, I., 2017). Common delivery techniques include phishing emails, supply chain attacks, drive-by downloads, and infected media such as malware-injected USB flash drives. In the context of government infrastructure, cyberattacks can threaten vital sectors such as energy, transportation, telecommunications, and healthcare. Successful attacks on these sectors can result in the disruption of essential services, economic losses, and threats to national security. A clear example of an attack reaching the delivery stage is the “Brain Cipher” ransomware incident that attacked Indonesia's National Data Center (NDC) on June 20, 2024 (Ma’ruf, S., 2024). This attack paralyzed vital public services and exposed security gaps in the country's digital infrastructure. To protect government infrastructure from threats at the delivery stage, several mitigation measures can be implemented. Cybersecurity awareness training is required so that employees can recognize attack tactics such as phishing and understand the importance of verifying the source of an email or link before interacting with it. Implementation of email security solutions, such as spam filters and malware detection, is also essential to prevent malicious emails from reaching employees' inboxes (Amin et al., 2024). In addition, strict policies regarding the use of external devices can help reduce the risk of malware infection via USB or other devices. Finally, regular system monitoring and software updates should be performed to detect suspicious activity and close security holes before they are exploited by attackers.

*D. Exploitation*

Exploitation is the fourth stage in the Cyber Kill Chain, where attackers utilize system vulnerabilities to gain or increase access. Common techniques used include software vulnerability utilization, SCADA attacks, phishing, and ransomware (Tarnowski, I., 2017). In government infrastructure, exploitation can have serious consequences, such as disruption of public services, leakage of sensitive data, and national security threats. For example, the “Brain Cipher” ransomware attack on June 20, 2024 paralyzed Indonesia's National Data Center (Ma’ruf, S., 2024). Mitigation efforts include periodic system updates, cyber awareness training, IDPS implementation, network segmentation, as well as regular security testing to prevent exploits and strengthen digital defense systems.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 49 No. 1 February 2025, pp. 663-672

*E. Installation*

Installation is the fifth stage in the Cyber Kill Chain, where the attacker implants malware or a backdoor into the target system to maintain long-term access. Success at this stage allows the attacker to remain hidden within the network, allowing them to steal data or launch further attacks against government infrastructure. Common techniques used include Trojan horses, exploitation of system vulnerabilities, malicious scripts and infected USB devices. If successful, these attacks can lead to disruption of public services, leakage of confidential data and threats to national security. To prevent and mitigate these risks, measures include regular system updates, cyber awareness training, and implementation of IDPS to detect threats early. In addition, strict policies regarding the use of external devices and regular system monitoring and auditing are essential to identify and remove malware before it can cause further damage (Couretas, J. M., 2022).

*F. Command and Control (C2)*

Command and Control (C2) is the sixth stage in the Cyber Kill Chain, where the attacker establishes a communication channel with the infected system to control the malware and direct further attacks. Success at this stage allows attackers to monitor, update and collect data from compromised systems, including government infrastructure that manages public services and sensitive data (Tarnowski, I., 2017). Common techniques used in C2 include hidden servers, cloud infrastructure utilization, encrypted communications, and steganography, all of which are designed to avoid detection by security systems. To prevent and mitigate this threat, steps that can be taken include real-time monitoring of network traffic, implementation of intrusion detection and prevention systems (IDPS), and implementation of strict security policies that restrict suspicious outbound communications. In addition, periodic system updates and cyber awareness training for employees are essential to detect signs of compromise and reduce the risk of attackers gaining control of the system (Baker, B., 2019).

*G. Actions on Objectives*

Actions on Objectives is the final stage in the Cyber Kill Chain, where the attacker has gained full access to the target system and begins to execute their goal. In the context of government infrastructure, these actions can have a major impact on operations and national security, including the theft of confidential data, sabotage of critical systems, and manipulation of information that can disrupt public policies and services. Some of the more common forms of attack at this stage include the theft of sensitive data, such as government documents or strategic intelligence that can be used for espionage or extortion (Bahrami et al., 2019). Additionally, attackers may sabotage systems that disrupt essential services, data tampering to mislead decision-makers, and spreading disinformation to sway public opinion. Another dangerous tactic is extortion using ransomware, which encrypts critical data and disrupts government operations until a ransom is paid. To prevent and address attacks at this stage, government agencies need to implement strict security policies, such as stronger access controls and real-time network monitoring. In addition, cyber awareness training for employees, periodic security testing to identify security gaps, and the development of incident response plans are essential in dealing with this threat. Collaboration between agencies, both at the national and international levels, is also needed to share information on the latest threats and effective defense strategies (Kim et al., 2019).

In the face of increasingly sophisticated cyber threats to government infrastructure, a comprehensive security strategy is required. One effective approach is the “zero trust” model, where every user, device and system is not immediately trusted before passing through a security verification process. This implementation includes strict access controls and layered authentication, ensuring only verified entities can access critical resources (Djenna et al., 2021). In addition, the utilization of artificial intelligence (AI) in security monitoring enables real-time detection of suspicious activities, so that threats can be responded to quickly (Li, Y., 2021).

Cooperation between government agencies is also a crucial factor in strengthening cybersecurity (Hohmann et al., 2017). One of the strategic steps taken is the establishment of Cyber Incident Response Teams (CSIRT) in various regions, such as the East Kalimantan Provincial Government (Suprojo et al., 2024). These teams are responsible for coordinating responses to cyber attacks, conducting forensic investigations, and providing preventive recommendations to avoid similar attacks in the future. Support from high-ranking officials and synergy between agencies are needed for this team to function optimally (Sarosa et al., 2023). In addition,

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 49 No. 1 February 2025, pp. 663-672

strengthening a secure and reliable information technology (IT) infrastructure is a fundamental aspect in maintaining government cybersecurity. Important steps include periodic risk evaluations, implementation of security layers such as firewalls and data encryption, and increased security awareness for government employees through training. Real-time system monitoring and the development of disaster recovery plans are also important to ensure operational continuity and reduce the impact of cyber incidents (Yaseen, A., 2020).

Finally, increasing the capacity of human resources (HR) in the field of cybersecurity should be a priority. The government can work with education and training institutions to upskill employees to deal with evolving cyber threats. Regular training and certification in information security will ensure that digital security professionals have adequate skills to effectively protect government assets.

TABLE I. STAGES OF TACTICS, TECHNIQUES, AND PROCEDURES (TTP) USED IN CYBERATTACKS AGAINST GOVERNMENT INFRASTRUCTURE

| Stages of Attack | Tactics | Techniques | Procedures |
|---|---|---|---|
| Reconnaissance | Gather information on targets to identify vulnerabilities. | Network scanning (network scanning), social engineering (phishing, pretexting), and OSINT (Open Source Intelligence). | Using tools like Nmap or Shodan, phishing via email or social media, and analyzing public data. |
| Weaponization | Create tools or payloads to exploit vulnerabilities. | Malware development (RAT, ransomware), creation of documents containing exploits (PDF, Word), and exploit kit usage. | Using frameworks like Metasploit, creating PDF/Word files containing malicious macros, and integrating exploits into attack tools. |
| Delivery | Deliver the payload to the target through various channels. | Phishing emails with malicious attachments, drive-by downloads from websites, and distribution via USB or physical media. | Sending emails with malware attachments, creating malicious websites that infect visitors, and deploying infected USBs to target locations |
| Exploitation | Exploit vulnerabilities to gain access to systems. | Exploitation of software vulnerabilities (zero-day, unpatched vulnerabilities), use of brute force or credential stuffing techniques | Using exploits like EternalBlue, executing brute force attacks on system logins, and leveraging vulnerabilities in web applications |
| Installation | Install malware or a backdoor to maintain access. | Installing RAT (Remote Access Trojan), creating a new user account, and using persistence techniques (registry, scheduled tasks) | Running a script to install malware, added a registry entry for persistence, and creating a task scheduler to run the malware |
| Command and Control (C2) | Establish a connection with the attacker's server to control the victim's system. | Uses protocols such as HTTP, DNS, or HTTPS for communication, uses domain generated algorithms (DGA), and uses tunneling techniques | Setting up C2 servers with tools such as Cobalt Strike, encrypting the communication between the malware and the server, and using DNS tunneling techniques to avoid detection |

| | | | |
|---|---|---|---|
| Actions on Objectives | Performing the goal of the attack, such as data theft or intrusion. | Data theft (data exfiltration), data encryption for ransomware, and data deletion or manipulation (wipe, tamper) | Using tools like Mimikatz to steal credentials, encrypts files or demands ransom, and executing commands to delete or corrupt data |

## V. CONCLUSION

This research takes an in-depth look at the Tactics, Techniques and Procedures (TTPs) used in cyberattacks against government infrastructure. Key findings highlight the importance of cross-agency collaboration and integration of advanced technologies to formulate effective mitigation strategies. An in-depth understanding of TTPs enables the development of policy recommendations that improve preparedness against evolving cyber threats, making government infrastructure security efforts more resilient and responsive to the dynamics of digital attacks. The study also emphasizes that cyberattacks against government infrastructure often involve a variety of sophisticated techniques, such as the collection of information through social engineering, the exploitation of software vulnerabilities, and the use of specialized malware designed to evade detection. In addition, such attacks can have significant impacts, including disruption of public services, theft of sensitive data and threats to national security. Therefore, a proactive approach to cybersecurity, including cyber awareness training for employees and the implementation of sophisticated intrusion detection systems, is necessary to protect critical government assets. As such, this research makes an important contribution to understanding and addressing cyber threats to government infrastructure, and offers practical guidance for policymakers and cybersecurity professionals in strengthening national digital defenses.

## ACKNOWLEDGMENT

The authors would like to thank the Republic of Indonesia Defense University, especially the Master of Cyber Defense Engineering Study Program, Faculty of Defense Science and Technology, for the academic support and research facilities provided. Appreciation is also expressed to the supervisors for their guidance and valuable input during the research process. Gratitude is also addressed to colleagues and parties who have contributed to the completion of this journal. Hopefully this research will be useful for the development of cyber defense science.

## REFERENCES

[1] Amin, K., Paramitha, D. I., Al Farauqi, M. D. A., & Shalehah, A. (2024). Managing Power Rivalry: Indonesia's Perspective and Strategy in Managing Relations with China in the Indo-Pacific. *ii Dynamics in the Indo-Pacific: From Geopolitics and Geoeconomics Perspectives*, 73.

[2] Andress, J., & Winterfeld, S. (2013). Cyber warfare: techniques, tactics and tools for security practitioners. Elsevier.

[3] 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.

[4] Bahrami, P. N., Dehghantanha, A., Dargahi, T., Parizi, R. M., Choo, K. K. R., & Javadi, H. H. (2019). Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures. Journal of information processing systems, 15(4), 865-889.

[5] Baker, B. (2019). An Analysis of Commonly Observed Command and Control TTPs (Master's thesis, Utica College).

[6] Chauhan, A. S. (2018). Practical Network Scanning: Capture network vulnerabilities using standard tools such as Nmap and Nessus. Packt Publishing Ltd.

[7] Clarke, D. (2019). Capacity Building for a Cybersecurity Workforce Through Hands-on Labs for Internet-of-Things Security. National Cyber Summit (NCS) Research Track, 1055, 14.

[8] Couretas, J. M. (2022). Cyber security and defense for analysis and targeting. In An Introduction to Cyber Analysis and Targeting (pp. 119-150). Cham: Springer International Publishing.

[9] Creswell, J. W. (2021). A concise introduction to mixed methods research. SAGE publications.

[10] Creswell, J. W., & Plano Clark, V. L. (2023). Revisiting mixed methods research designs twenty years later. Handbook of mixed methods research designs, 1(1), 21-36.

[11] Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. Land Forces Academy Review, 26(1), 69-75.

[12] Diogenes, Y., & Ozkaya, E. (2019). Cybersecurity–Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals. Packt Publishing Ltd.

[13] Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10), 4580.

[14] Edy, S., Gunawan, W., & Wijanarko, B. D. (2017, November). Analysing the trends of cyber attacks: Case study in Indonesia during period 2013-Early 2017. In 2017 International Conference on Innovative and Creative Information Technology (ICITech) (pp. 1-6). IEEE.

[15] Evangelista, J. R. G., Sassi, R. J., Romero, M., & Napolitano, D. (2021). Systematic literature review to investigate the application of open source intelligence (OSINT) with artificial intelligence. *Journal of Applied Security Research*, *16*(3), 345-369.

[16] Hohmann, M., Pirang, A., & Benner, T. (2017). Advancing Cybersecurity Capacity Building. Global Public Policy Institute (GPPi).

[17] Khan, M. S., Siddiqui, S., & Ferens, K. (2018). A cognitive and concurrent cyber kill chain model. Computer and Network Security Essentials, 585-602.

[18] Kim, H., Kwon, H., & Kim, K. K. (2019). Modified cyber kill chain model for multimedia service environments. Multimedia Tools and Applications, 78, 3153-3170.

[19] Larasati, H. T., & Haryadi, S. (2016, August). Basic planning of data center infrastructure and bandwidth requirement in integrated government network. In *2016 2nd International Conference on Wireless and Telematics (ICWT)* (pp. 117-121). IEEE.

[20] Lee, N. (2024). Cyberattacks, Prevention, and Countermeasures. In Counterterrorism and Cybersecurity: Total Information Awareness (pp. 295-342). Cham: Springer International Publishing.

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

[22] Ma'ruf, S. (2024). Crisis Management and Incident Response: A National Data Center Case Study. Jurnal Intelek Dan Cendikiawan Nusantara, 1(3), 4619-4633.

[23] Pliatsios, D., Sarigiannidis, P., Lagkas, T., & Sarigiannidis, A. G. (2020). A survey on SCADA systems: secure protocols, incidents, threats and tactics. IEEE Communications Surveys & Tutorials, 22(3), 1942-1976.

[24] Ramadhianto, R., Rezasyah, T., Kertopati, S. N. H., Estrada, M. A. R., & Kanellopoulos, A. N. (2024). Strengthening management of non-military intelligence organizations in detecting cyber threats to support national security. Bakti Garuda Journal, 1(1), 89-120.

[25] Sarosa, W., Susetyo, N. A., Aulianisa, M. N., Maulaa, M. R., & Giffary, P. (2023). Fostering Human Dimension Of Smart Cities: Lessons from Jakarta for Nusantara, Indonesia's New Capital City in the Making. Smart City, 2(2), 4.

[26] Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (idps). NIST special publication, 800(2007), 94.

[27] Sfetcu, N. (2024). Advanced persistent threats in cybersecurity–Cyber warfare. MultiMedia Publishing.

[28] Suprojo, B., Salim, M. N., Wicaksono, A., Prihatin, S. M., Purbawa, Y., Prayoga, R. A., ... & Wahyono, E. (2024). Improving Quality of Land Data Towards Modern Land Administration in The Administrative City of West Jakarta. Journal of Government and Civil Society, 8(2), 204-227.

[29] Tarnowski, I. (2017). How to use cyber kill chain model to build cybersecurity?. European Journal of Higher Education IT.

[30] Yaseen, A. (2020). Uncovering evidence of attacker behavior on the network. ResearchBerg Review of Science and Technology, 3(1), 131-154.

[31] Yulianto, A. (2021). Cybersecurity policy and its implementation in Indonesia. Law Research Review Quarterly, 7(1), 69-82.