Formosa Journal of Applied Sciences (FJAS)
Vol. 4, No.2 2025: 615-626

The Indonesia's Cyber Security Strategy in the Face of Evolving Modern Warfare Threats

Ria Wulandari[1*], Priyanto[2], Afrizal Hendra[3]
Universitas Pertahanan Republik Indonesia
Corresponding Author: Ria Wulandari riawulandhari@gmail.com

A R T I C L E I N F O

Keywords: Cybersecurity, Modern Warfare, Threats, Strategy

Received : 21, December
Revised : 23, January
Accepted: 25, February

©2025 Wulandari, Priyanto, Hendra: This is an open-access article distributed under the termsof the Creative Commons Atribusi 4.0 Internasional.

A B S T R A C T

This research explores Indonesia's strategy to address the threat of modern warfare, specifically cyberattacks that jeopardize the country's sovereignty. The focus is on the TNI Cyberforce, which was established to counter the increasing cyber threats since 2023. Indonesia has faced data leaks, ransomware attacks and espionage targeting vulnerable IT infrastructure. These attacks are used for intelligence theft, manipulation of public opinion, and disinformation by foreigners. TNI Cyberforce aims to strengthen national security, restore public trust, and improve readiness. This qualitative study uses a literature review and an objectives-ways-means framework to analyze the role of the Cyberforce as well as the human resources and infrastructure required. As part of Indonesia's defense strategy, the TNI Cyberforce plays an important role in maintaining sovereignty in the digital era.

DOI prefik: https://doi.org/10.55927/fjas.v4i2.5
ISSN-E: 2962-6447
https://srhformosapublisher.org/index.php/fjas

INTRODUCTION

Modern warfare today is not only limited to physical combat, but also includes digital aspects that greatly affect the political, economic and social stability of a country. Cyberthreats have become one of the new forms of war used by certain countries or groups to access, damage, or alter the strategic data of the opposing country without having to deploy conventional forces. Indonesia, as a country with the world's fourth largest population and a rapidly growing economy. It is a prime target for cyberattacks aimed at damaging critical infrastructure, stealing sensitive data, or manipulating public opinion.

In 2023, the National Cyber and Crypto Agency (BSSN) recorded a total anomalous traffic of 403,990,813, which is an indicator of cyber attacks that threaten Indonesia's security system (BSSN, 2023). The anomalous traffic, which came from various threat sources, showed the potential for data leakage, hacking, and disruption to the country's critical infrastructure. One major incident that occurred was the hacking of the Indonesian Ministry of Defense website on November 1, 2023, which resulted in 667 users and the personal data of 37 employees being leaked (Tempo, 2023). This hack involved the use of malware stealer, software specifically designed to steal personal and sensitive data (Ilker, 2021). For this reason, it is necessary to strengthen institutions The Indonesian National Armed Forces (TNI) that handle cybersecurity, such as the establishment of the TNI Cyberforce, which is a strategic solution in overcoming this threat. This research aims to explore how the establishment of TNI Cyberforce can improve national preparedness in the face of cyberattacks, as well as who will be recruited as members to fill the position.

On November 1, 2023, the website of the Ministry of Defense of the Republic of Indonesia (Kemhan RI) was hacked by hackers who used a malware stealer device to steal important data. BSSN (National Cyber and Crypto Agency) revealed that this hack is part of the growing cyberthreats to the country's digital infrastructure. The data stolen by the hackers, including users' personal information, was then sold and published on the BreachForums website (Kompas, 2023). This incident raises concerns about the vulnerability of Indonesia's cyber defense system, which not only threatens security aspects, but can also affect the country's political and economic stability. This kind of cyberattack is increasingly becoming a serious threat, which reminds the importance of protecting the country's data and information systems. To deal with this, the Indonesian government has issued a number of regulations, such as the ITE Law No. 11 of 2008 which was revised by Law No. 19 of 2016, as well as Law No. 27 of 2022 on Personal Data Protection, which aims to strengthen the digital security system and protect personal data from misuse of technology.

The current regulations have an important role in providing protection for personal data and addressing cybercrime. The ITE Law No. 11 of 2008 is the main foundation in dealing with cybercrime, while the Personal Data Protection Law (PDP) No. 27 of 2022 is very relevant in overcoming data leakage problems, such as what happened to the Indonesian Ministry of Defense. For this reason, Kemhan RI needs to strengthen regulations and digital defense systems in order to prevent and overcome cyberthreats in the future. The ITE Law and PDP Law become an important legal umbrella in overcoming cyberthreats, as well as the basis for the formation of the TNI Cyberforce consisting of Cybersecurity Engineers. The establishment of TNI Cyberforce is expected to strengthen Indonesia's cyber resilience, with the strategy explained using the ends-ways-means framework, to explain the relationship between the ends, ways, and means needed in dealing with increasingly complex cyberthreats. This research will begin by compiling a title, abstract, introduction, research methods, and continue with results and in-depth discussions related to the role of TNI Cyberforce in maintaining state sovereignty.

LITERATURE REVIEW

Modern warfare today is not only limited to physical combat, but also includes digital aspects that greatly affect the political, economic and social stability of a country. Potential for data leakage, hacking, and disruption to the country's critical infrastructure. One major incident that occurred was the hacking of the Indonesian Ministry of Defense website on November 1, 2023, which resulted in 667 users and the personal data of 37 employees being leaked (Tempo, 2023). The current regulations have an important role in providing protection for personal data and addressing cybercrime. The ITE Law No. 11 of 2008 is the main foundation in dealing with cybercrime, while the Personal Data Protection Law (PDP) No. 27 of 2022 is very relevant in overcoming data leakage problems, such as what happened to the Indonesian Ministry of Defense.

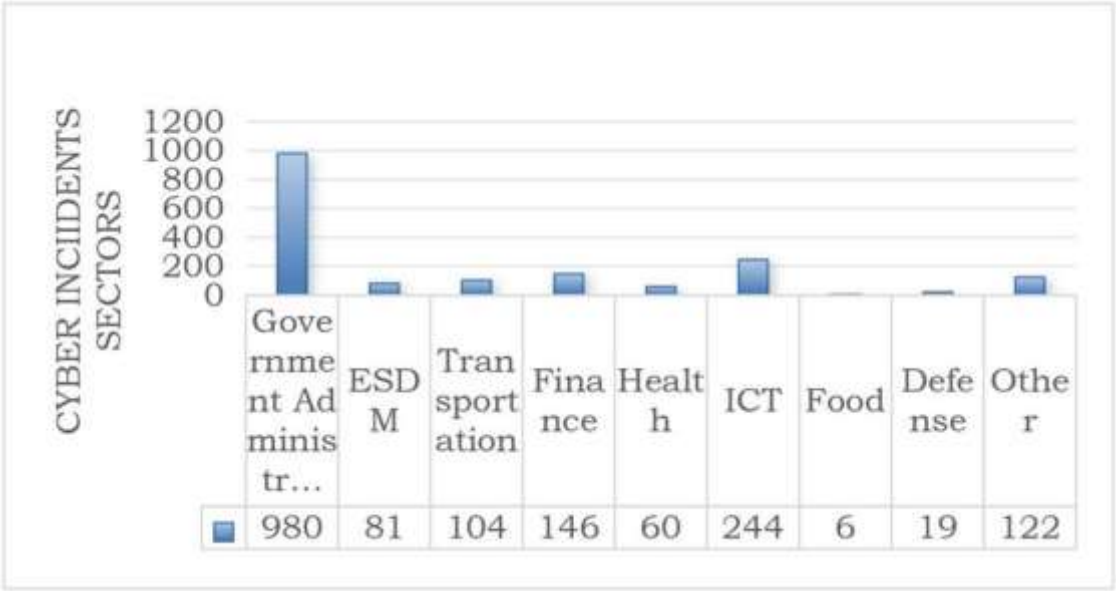
METHODOLOGY

This research uses a comprehensive descriptive qualitative method, with text analysis of a bibliography that includes books, articles, journals, and mass media as the main source. The approach used is a literature study that focuses on understanding the process, meaning and context related to the issue of cyberthreats and Indonesia's defense strategy. Data was collected through interview techniques, observation, and document analysis to provide a more in-depth picture of existing cyber defense policies and strategies. This article discusses how Indonesia developed a cyber security strategy to deal with the evolving threats of modern warfare.

RESEARCH RESULT

On November 1, 2023, the Indonesian Ministry of Defense website was hacked by hackers, indicating a serious threat to cybersecurity in Indonesia (BSSN, 2023). The hacker used a malware tool, more specifically a type of malware stealer, which successfully accessed and stole important data (Kompas.com, 2023). Personal data of employees at the Indonesian Ministry of Defense, including other sensitive information, was leaked due to this hack (Kompas.com, 2023). In addition, the hackers also uploaded the stolen data to the BreachForums website, which made the situation worse as the stolen data could be misused by irresponsible parties (Kompas.com, 2023). This adds to the risk of greater cybercrime, ranging from extortion to potential threats to state sovereignty (Akram, 2023). The threat posed by data leaks can be used for public manipulation, espionage, and disinformation, further undermining trust in Indonesia's defense system (Buku Putih, 2015). The following is data on cyberattack incidents in various sectors:

Table 1. Number of Cyber Incidents Attacking Several Institutional Sectors (BSSN, 2023).



From the table above, the data shows that cyberattacks on state administration are the highest. While in the defense sector there were 19 times. The defense sector is one of the most vital sectors in maintaining the integrity and sovereignty of the state. Although attacks on the defense sector do not occur frequently, such events can undermine public and other countries' confidence in Indonesia's ability to protect itself. This can impact national political and economic stability. In addition, the defense sector has many interconnected critical infrastructures, such as military communication networks, air defense systems, and military logistics and supply systems. An attack on this infrastructure could cause widespread damage to the country's operational readiness.

The most detected cyber incidents occurred in the government administration sector, with 980 cases recorded in 2023. This sector has a very crucial role in running the wheels of government and public services, making it a prime target for cyberattacks that can disrupt the smooth running of state administration. Attacks targeting the government administration sector have the potential to cause critical data leaks, system manipulation, and damage public trust in government institutions. Therefore, it is important to strengthen the cybersecurity system in this sector with stricter regulations, as well as strengthening infrastructure and increasing the capacity of human resources in charge of keeping government data and systems safe and protected from increasingly complex threats. In addition to the government administration sector, the Information and Communication Technology (ICT) sector also experienced significant cyber incidents, with 244 cases recorded in 2023.

The ICT sector is an easy target for hackers due to its vital role in supporting various other sectors, including government, economy, and defense.Its vulnerability to cyberattacks can damage critical communication infrastructure, such as internet networks, telecommunications, and inter-agency communication systems. Cyberattacks in the financial sector were also recorded in 146 cases, which had a direct impact on financial losses and leakage of customer data, threatening economic stability.In the transportation sector, 104 cyber incidents were recorded, causing disruptions to air, sea, and land transportation systems, potentially disrupting mobility and safety.Given this high threat, vital sectors such as state administration, ICT, finance, and transportation require intensive strengthening of cyber defense systems to maintain national stability and security.

The threat of malware, especially in the form of Generic Trojan RATs, is increasing. This shows the importance of a deep understanding of how malware works to protect systems from damage. Malware, as explained by Alomari (2024), is software that is intentionally designed to damage or illegally access systems, causing great harm to individuals and organizations. Generic Trojan RAT, which targets computers with Windows operating systems, is one of the most common types of malware used in cyberattacks (BSSN, 2023). These attacks are often spread through social engineering methods, which take advantage of user negligence or ignorance in handling suspicious emails or files. One of the techniques used is Phishing Site, which is an activity that infects the system by tricking the victim into visiting a malicious site. For example, the attack that occurred on the Indonesian Ministry of Defense website in 2023 involved Trojan-type malware that successfully stole sensitive data. This confirms the importance of strengthening the cyber defense system, as reflected by the need to tighten digital security regulations in Indonesia. The government should adopt the latest technologies, such as intrusion detection systems (IDS) and firewalls, to detect and prevent future cyberattacks.

DISCUSSION

Based on BSSN data on anomalous traffic, in 2023 Generic Trojan RAT will attack the most. The establishment of TNI Cyberforce aims to maintain the country's sovereignty from cyber threats. The establishment of TNI Cyberforce is in line with the government's efforts to strengthen regulations that support cybersecurity, such as the ITE Law (Law No. 11 of 2008), Personal Data Protection Law (Law No. 27 of 2022), and Law No. 3 of 2002 on National Defense. The establishment of TNI Cyberforce is a strategic step to safeguard Indonesia's sovereignty from increasingly complex cyber threats. With the background of Law No. 3 of 2002 on National Defense, TNI Cyberforce aims to strengthen regulations that support the country's cyber security (Hasan, 2022). Cyberwarfare can cause unrest in society if it escalates quickly because it has the potential to steal state secret information (Soewardi, 2013). Currently, the TNI already has small units in handling cyber threats such as the organization of the TNI Cyber Unit, Pussansiad TNI AD (Pusat Sandi dan Siber Angkatan Darat /Army Cyber and Crypto Center), Libpam Sisjar TNI AL (Dinas Pengamanan dan Siber Jaringan Angkatan Laut/Navy Network Security and Cyber Unit), and Satsiber TNI AU (Satuan Siber Angkatan Udara/Air Force Cyber Unit). Special units for cyber forces have been established in various countries (Hasan, 2022). Indonesia needs to cooperate with cybersecurity agencies such as the U.S. Cyber Command and China's Strategic Support Force. Then, the need for a well-coordinated cyber defense, cyber units in each of the TNI dimensions, namely the Army, Navy, and Air Force, can be more effective if they are combined and integrated into one unit in the TNI Cyberforce. The following anomalous traffic data is the reason why TNI Cyberforce should be formed immediately:

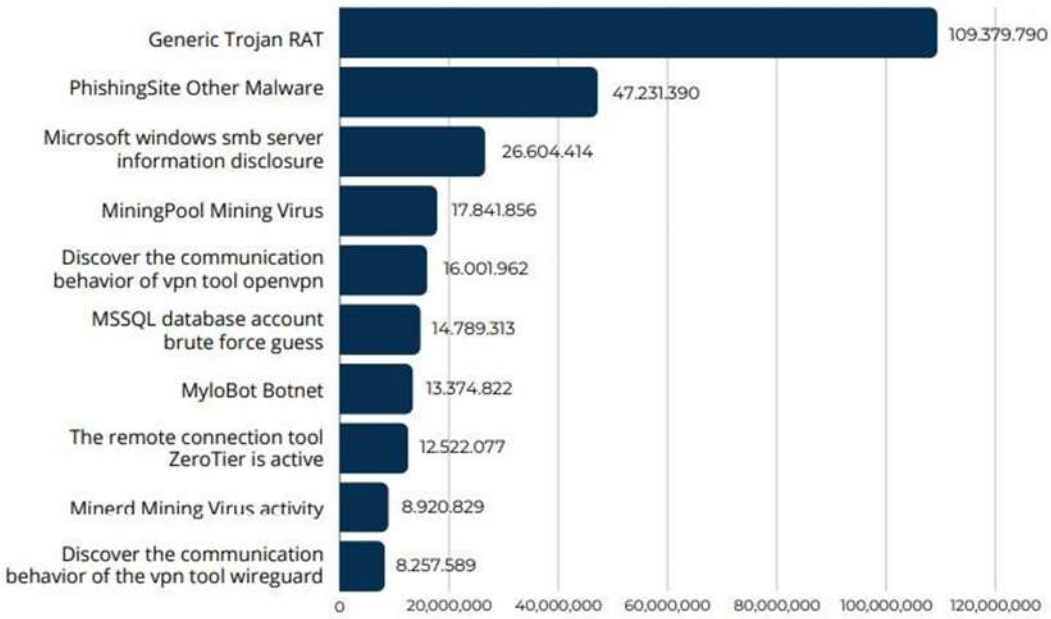


Figure 1. Anomalous Traffic Data (BSSN, 2023)

There is a list of threats with quantitative values for the amount of traffic associated with the threat. Some of the major threats are:

a. Generic Trojan RAT: was the biggest threat with a traffic value of 109,379,790.
b. Phishing Site Other Malware: had traffic of 47,231,390.
c. Microsoft Windows SMB Server Information Disclosure: traffic amounted to 26,604,414.
d. Mining Pool Mining Virus: traffic of 17,841,856.

The he establishment of TNI Cyberforce is a vital strategic step to protect the country's sovereignty in the digital era, given the increasing complexity of cyberthreats that can damage the country's vital infrastructure. For this reason, a structured approach and adequate resources are needed, including recruiting Cybersecurity Engineers who have expertise and experience in dealing with cyberthreats. In addition, it is important to upgrade the required technology, both software and hardware, to ensure readiness in dealing with evolving cyberattacks. This effort must be fully supported, given the increasingly sophisticated and far-reaching cyber threats. TNI Cyberforce is part of the government's strategy to maintain state sovereignty, with implementation based on existing regulations, such as ITE Law No. 11 of 2008 and PDP Law No. 27 of 2022.

The recruited Cybersecurity Engineers have the ability to prevent and early detect cyberattacks, and are proficient in using the latest technology, such as intrusion detection systems (IDS), firewalls, encryption, and anomaly detection, which are very important in maintaining national security. Cybersecurity Engineers are individuals who are instrumental in protecting data from cyberthreats by identifying potential vulnerabilities and securing vulnerable information systems (Perrin, 2020). The profession encompasses a wide range of disciplines, including cryptography, which is at the core of digital data protection (Easttom, 2022). In the era of the Military Internet of Things (MIoT), where military operations can be remotely controlled with speed and precision, the competence of Cybersecurity Engineers is becoming increasingly crucial (Indonesia.go.id). Only internationally certified individuals such as CEH, CISSP, or CISM are able to fulfill the high demand for cybersecurity (Perrin, 2020). In comparison, Singapore has established the Digital and Intelligence Service (DIS) to handle modern digital and intelligence threats (MINDEF Singapore). To keep pace with this progress, the TNI Cyberforce is projected to require 500-1,000 expert personnel who are competent in supporting the strategic needs of national security in cyberspace.

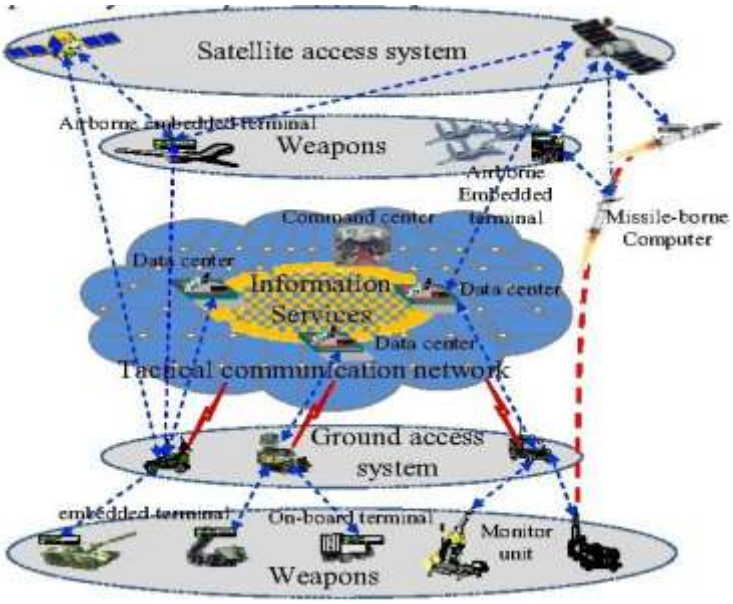


Figure 2. Internet of Things (IoT) Applications in the Military (IOTM). (Yushi, 2012)

An explanation of Figure 2 which discusses military Internet of Things (IoT) applications, or what is referred to as the Military Internet of Things (MIOT) as follows:

a. Satellite Access System:
   Connects communication systems with satellites to provide remote access. Used to support communication to airborne embedded terminals, command centers, and data centers.
b. Airborne Embedded Terminal:
   Part of an airborne weapon system such as a fighter aircraft or drone connected to a tactical communications network.
c. Information Services:
   The central element in the MIOT system. It acts as an integration platform to store, process, and distribute data over the communication network.
d. Data center serves as the main node to support information services.
e. Tactical Communication Network:
   Connects various MIOT elements, including the data center, command, and integrated terminals. Ensures data can be transmitted securely between elements.
f. Ground Access System:
   A ground-based communication system that supports embedded terminals in military vehicles and monitor units.
g. Weapons:
   Includes ground and air-based weapon units connected to the MIOT to provide rapid response through real- time data and communications. Includes missiles with onboard computers for direct control.

Communication Lines:

a. Dotted Blue Line:
   Indicates the main communication path through satellite access and tactical communication networks.
b. Red Line:
   Representation of critical data flows, such as missile control or weapon response.

Key MIOT Functions:

a. Data Integration:
   Enhances system capability by combining data from ground, air and satellite.
b. Real-Time Response:
   Accelerates data-driven decision- making on the battlefield.
c. Multi-level Connectivity:
   Connects various military systems at strategic and tactical levels.

Cybersecurity is part of various disciplines, one of which is cryptography, which plays an important role in protecting data and communication in the digital world (Easttom, 2022). Individuals who have international certifications such as CEH, CISSP, or CISM have high competence in this field, which allows them to face complex security challenges (Perrin, 2020). Along with the advancement of technology, the world is now entering the era of the Military Internet of Things (MIoT), which refers to the application of IoT technology in the military field. MIoT involves a network of interconnected military devices, providing a great opportunity to improve national defense capabilities by connecting critical elements such as central command, vehicles, and personnel. With drones, robots, and naval vessels equipped with MIoT technology, attack missions can be carried out more effectively. In addition, MIoT also helps in detecting and responding to unconventional threats. However, the threat of cyberattacks can weaken the MIoT system, so strong protection is needed. With 5G support, MIoT's capacity to share data in real-time will increase, making it an effective military tool equipped with an MIOT system in dealing with global threats.

Cybercrime often occurs because of the interests of certain individuals or groups that aim to harm other parties or personal (Rahmawati, 2017). In the face of this threat, securing files and protecting vital objects are the main concerns in cybersecurity (Soesanto, 2023). The Indonesian government, through the Indonesian Ministry, has full authority in the formation of a cyber army, which aims to protect the country's sovereignty from cyberthreats (Hasan, 2022). The recruitment process of the cyber army can be done through various methods, with evenly distributed deployment throughout Indonesia to ensure comprehensive national security (Hasan, 2022). TNI Cyberforce, in collaboration with Cybersecurity Engineers, plays an important role in strengthening digital security, with the support of modern technologies such as 5G networks and Military Internet of Things Military (MIOT) devices, which increase the effectiveness of defense against global cyberthreats.

CONCLUSIONS AND RECOMMENDATIONS

Indonesia's strategy in dealing with increasingly complex cyber threats centers on the Indonesian National Armed Forces (TNI) specifically to handle cyber security, in this case the formation of the TNI Cyber Force. TNI Cyberforce as the main solution to protect the country's sovereignty. With the rise of threats such as the theft of confidential data and espionage, the TNI Cyberforce is formed from personnel who have special expertise involving TNI cyber units from Pussansiad TNI AD (Pusat Sandi dan Siber Angkatan Darat /Army Cyber and Crypto Center), Dinas Pengamanan dan Siber Jaringan Angkatan Laut (Libpam Sisjar TNI AL/Navy Network Security and Cyber Unit), and Satuan Siber Angkatan Udara (Satsiber TNI AU/Air Force Cyber Unit) including Cybersecurity Engineers. The recruitment of these personnel is followed by inter-agency collaboration, such as the Ministry of Defense, BSSN, and other agencies, to strengthen national coordination. Strengthening regulations, such as ITE Law No. 11 of 2008 and PDP Law No. 27 of 2022, is a relevant legal basis to support this strategy. In addition, Indonesia can learn from other countries' strategic approaches in building a resilient cyber defense system. Modern technology support, such as 5G networks, Military Internet of Things (MIoT), and systems such as Intrusion Detection Systems (IDS), play an important role in dealing with global threats. With the synergy between these components, TNI Cyberforce is expected to be the main pillar in protecting the country's vital infrastructure from cyberattacks.

ADVANCED RESEARCH

What are the risks and mitigations to dependence on foreign technology in supporting cyber operations, especially satellites. This is because reliance on foreign technology has the potential to make the country vulnerable to political or diplomatic pressure from the country providing the technology. This could include termination of technology access or restrictions on certain uses, which could disrupt critical operations such as satellite communications or intelligence. Enhancing domestic technological capabilities, such as the ability to build and operate satellites, as well as local cyber defense systems, will provide autonomy and reduce the risk of dependency.

ACKNOWLEDGMENT

I would like to express my heartfelt thanks to Mr. Prabowo Subianto, President of the Republic of Indonesia, who has provided an executive master's scholarship program. Also my colleagues, for their invaluable suggestions and feedback during the course of this research. Their expertise and insight have been instrumental in shaping the direction of this paper. I also wish to acknowledge the financial support provided by Republic Indonesia Defense University and The Indonesian Ministry of Defence, which made it possible to complete this study. Without their generous assistance, this research would not have been feasible. Finally, I would like to thank my parents and my best lecturers for their continuous encouragement and support.

REFERENCES

Akram, F. (2023). Implementasi Password Stealing Attack Terhadap Saved Password Pada Browser Komputer Menggunakan Digispark Attiny85. Info Kripto, 17(1), 7-14.

Alomari, E., Nuiaa, R.R., Alyasseri, Z.A., Mohammed, H.J., Sani, N.S., Esa, M.I., & Musawi, B.A. (2023). Malware Detection Using Deep Learning and Correlation-Based Feature Selection. Symmetry, 15, 123.

Arianto, A. R., & Anggraini, G. (2019). Membangun pertahanan dan keamanan siber nasional Indonesia guna menghadapi ancaman siberglobal melalui Indonesia security incident response team on internet infrastructure (ID-SIRTII). Jurnal Pertahanan dan Bela Negara, 9(1), 13-30.

Arifin, M., & Kurniawan, R. (2022). Strategi Pengamanan Siber dalam Pertahanan Negara: Studi Kasus Pembentukan TNI Cyberforce. Jurnal Keamanan Nasional, 8(2), Pages: 123–140. https://doi.org/10.1234/jkn.v8i2.5678

ASEAN. (2023). ASEAN Cybersecurity Cooperation Strategy (2021 – 2025). ASEAN Cybersecurity Cooperation.

Badan Siber dan Sandi Negara (BSSN). (2022). Laporan Tahunan Keamanan Siber Indonesia. BSSN

Badan Siber dan Sandi Negara (BSSN). (2023). Lanskap Keamanan Siber Indonesia. BSSN.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications Asia-PacificPte. Ltd.

Dan-Marian, UNGUREANU; Alexandru-Lucian CUCINSCHI. (2022). CyberNSOF – A Crucial Force Multiplier In Modern Warfare. Vol 18 N0. 1. DOI: https://doi.org/10.53477/2971-8813-22-44

Digital and Intelligence Service (DIS) Singapura: Ministry of Defence Singapore. (2022). Digital and Intelligence Service

Easttom, C. (2022). Computer security fundamentals (4th ed.). Pearson Education.

Eurasia Review. (2024, December 20). Battling cyber warfare: Securing Indonesia's digital future. Eurasia Review. Retrieved from https://www.eurasiareview.com/20122024-battling-cyber-warfare-securing-indonesias-digital-future-oped/

Fadhila, A. (2024). Pemerintah memiliki regulasi yang bisa memperkuat keamanan digital. Jakarta: Kementerian Komunikasi dan Informatika.

Hasan, K.E. (2022). Perlunya Tentara Nasional Indonesia Memiliki Angkatan Siber Guna Menghadapi Era Cyber warfare. Journal of Education, Humaniora and Social Sciences (JEHSS).

Kara, Ilker. (2019). A basic malware analysis method. Computer Fraud & Security. Issue 6. Pages 11-19. https://doi.org/10.1016/S1361-3723(19)30064-8

Kementerian Pertahanan Republik Indonesia. (2015). Buku Putih Pertahanan. Kemhan RI.

Kompas.com. (2023). Hacker menyerang situs Kemhan RI dan menjual data di BreachForums.

Nugroho, F., & Wahyudi, H. (2021). Tantangan dan Peluang Pembentukan TNI Cyberforce di Era Digital. Jurnal PertahanandanKeamanan, 1 (3), 245 – 260. https://doi.org/10.1234/jpk.v10i3.7890

Nugroho, T. (2021). Strategi Nasional Keamanan Siber di Era Digital. Jakarta: Pustaka Komunikasi.

Portal Informasi Indonesia. (2024). Pentingnya Angkatan Siber dalam Era Military IoT. Indonesia.go.id.

Pratama, A., & Dewi, R. (2020). Membangun Pertahanan Siber: Perspektif Pembentukan TNI Cyberforce sebagai Garda Terdepan Keamanan Digital Indonesia. Indonesian Defense Journal, 4(2), 98–112. https://doi.org/10.1234/idj.v4i2.6789

Priyanto, D. (2021). Peran Badan Siber dan Sandi Negara dalam Keamanan Nasional. Jakarta: Lembaga Keamanan Siber.

Putri, A.W., Aditya, A.R., Musthofa, D.L., & Widodo, P. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator). Global Political Studies Journal.

Rahmawati, I. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense. Jurnal Pertahanan & Bela Negara Universitas Pertahanan RI.

Tempo. (2023). Situs Web Kemenhan Dibobol, Pakar Siber: Data Pribadi 667 User dan 37 Karyawan Bocor. https://www.tempo.co/ekonomi/situs-web-kemenhan-dibobol- pakar-siber-data-pribadi-667-user-dan-37-karyawan-bocor- 125351

Undang-Undang (UU) Nomor 3 Tahun 2002 adalah UU tentang Pertahanan Negara.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang. Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Universitas Pertahanan Republik Indonesia. (2021). Rektor Universitas Pertahanan RI : Internet Of Things (IoT) Mengubah Peperangan Modern. UNHAN RI.

Yushi, L., Fei, J., & Hui, Y. (2012). Study on Application Modes of Military Internet of Things (MIOT). IEEE International Conference on Computer Science and Automation Engineering (CSAE), 3, 630-634.