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

https://ijpsat.org/
Vol. 48 No. 1 December 2024, pp. 451-461

Building The Tni's Defense Posture In Cyberspace: Strategies For Dealing With Cyber Warfare In The Digital Era

Fauzi Abdurrachman[1], Bambang Suharjo[2], Yudhi Biantoro[3]

[1]Republic of Indonesia Defense University,

Bogor, West Java, Indonesia; fauziabdurrachman@tp.idu.ac.id [1]

[2,3]Republic of Indonesia Defense University,

Bogor, West Java, Indonesia; bambang_suharjo@tnial.mil.id [2]

Abstract – Cyber warfare is a growing strategic threat to national defense, particularly affecting the Indonesian National Armed Forces (TNI). With over 1.7 million cyberattacks targeting Indonesia's defense sector in 2022, enhancing the TNI's cyber defense posture is imperative. This study analyzes critical threats to TNI, examines advanced technologies such as blockchain, artificial intelligence (AI), and big data analytics, and proposes strategic measures tailored to Indonesia's context. A qualitative approach with descriptive analysis and global case studies (e.g., US, Russia, South Korea, and Estonia) was utilized to derive insights. Key findings highlight the importance of integrating rapid response units, the SMRD framework, and cyber deception tactics to improve threat detection and mitigation. Cross-sector collaboration and international partnerships are essential for achieving robust cyber resilience. The proposed strategies are expected to strengthen TNI's adaptive capacity in facing dynamic global cyber threats, ensuring national security in the digital era.

Keywords – Cyber warfare, TNI, artificial intelligence, cyber resilience, blockchain, big data analytics, national defense strategy, cyber deception, cross-sector collaboration.

1. INTRODUCTION

Modern warfare now extends to the cyber world where countries compete for control of information, disrupt critical infrastructure, and threaten national integrity. According to data collected by the State Cyber and Cryptography Agency (BSSN), in 2022 with a total of 84.8 million cyberattacks, Indonesia is the country with the highest number of cyberattacks in Southeast Asia. Of these, the defense sector was recorded to have experienced 1.7 million attacks (Honeynet, BSSN, 2022). This condition reflects significant vulnerabilities in national cyber defense systems, especially when compared to the capacity of developed countries that already have advanced technological infrastructure and artificial intelligence-based early detection strategies. Cyber warfare is asymmetrical, anonymous, and can be waged at a lower cost than conventional warfare. Cyber threats to national defense in this situation are becoming increasingly real and complex. As the main guardian of national sovereignty, the TNI faces a major challenge to adapt its defense strategy against increasingly complex digital threats. Study conducted by Hugyik (2020) and Oh et al., (2024) emphasized the importance of the military's ability to adapt to cyber threats, especially by using information and communication technology (ICT). The experience of South Korea and Russia shows that the use of new technologies, such as big data analytics and artificial intelligence (AI), can improve the effectiveness of cyber threat detection and deterrence.

The threat of cyber warfare has great potential to disrupt military infrastructure, weaken economic stability, and damage social order. Cyberwarfare has great potential to weaken defenses by attacking communication systems, logistics networks, and

command centers. Study by Baloch (2019) shows that the asymmetrical nature of cyber warfare allows non-state actors, such as terrorist or criminal groups, to become a major threat to national security. The increasing reliance on digital infrastructure in various industries, including defense and security, makes this threat even more relevant, especially for Indonesia. In addition, research by Candra et al (2021) and Azzani (2024) found that Indonesia faces challenges in building a cyber defense framework, including limited human resources trained in cyberspace, lack of investment in cutting-edge technology, and lack of adaptive regulations to dynamic cyber threats. To achieve this goal, an integrated and technology-based strategy is needed to strengthen military defense capabilities in cyberspace. Indonesia also needs to develop more adaptive regulations against cyber threats, including strategic data protection policies, minimum security standards for military systems, and a framework for collaboration between the government, the private sector, and the international community

This research focuses on efforts to build a tough, adaptive, and responsive cyber defense posture to cyber warfare threats. The main objectives of this study are to analyze cyber threats relevant to TNI defense operations, find cyber technologies that can be used to support TNI defense operations, and create strategies to strengthen TNI's cyber defense posture in cyberspace. This research is important because cyber warfare not only has an impact on military infrastructure, but also on the social and economic stability of a country. Study by Sholikah et al. (2024) shows that cyber warfare has become a major problem for national resilience, including for the TNI which plays an important role in maintaining Indonesia's territorial integrity.

Different from previous studies, this study offers a technology-based approach by integrating learning from developed countries such as the United States, Russia, South Korea, and Estonia, to provide a strategic framework that is relevant to the needs of Indonesia, especially the TNI. By utilizing technologies such as *big data analytics*, artificial intelligence *(AI),* and *blockchain*, the TNI is expected to be able to maintain national stability and sovereignty in the midst of evolving global threat dynamics.

2. LITERATURE REVIEW

Definition of Cyber Warfare and Its Relevance to National Defense

Cyber warfare is a form of modern conflict that uses information technology to attack computer systems or networks with the aim of weakening the operational functions of the target (Fedotenko, 2023). In contrast to conventional warfare, cyber warfare is asymmetrical, anonymous, and involves state and non-state actors. In addition to attacking digital infrastructure, cyber warfare can also undermine social stability through propaganda and information manipulation. According to Rudin et al., (2023), the Republic of Lithuania pays close attention to fifth-generation warfare, which uses asymmetric strategies and cyber technologies. To deal with this threat, the country has created a security framework based on cross-sector collaboration, which is relevant for the TNI in safeguarding national sovereignty.

Study by Baloch (2019) highlighting that cyber warfare has the potential to be used as an inexpensive yet effective strategic tool in attacking critical infrastructure, including military networks. Cyberwarfare allows perpetrators to carry out attacks without using physical force. Candra et al. (2021) also emphasized that Indonesia faces major challenges in strengthening cyber defense, including:

- Limited competent human resources,
- Lack of investment in advanced technology,
- Less adaptive regulation to dynamic threats.

This condition shows that the TNI needs to build an integrated and technology-based cyber defense strategy to protect military networks while maintaining national stability in the digital era.

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

https://ijpsat.org/
Vol. 48 No. 1 December 2024, pp. 451-461

Cyber Technology as a Threat Detection and Mitigation Tool

Modern technology plays a crucial role in improving cyber resilience. *Artificial Intelligence (AI)*, for example, enabling real-time threat analysis and automated response through the *Security Orchestration, Automation, and Response* (SOAR).Gustina DM (2024) explaining through *Security Orchestration, Automation, and Response* (SOAR), AI enables analytics *Real-time* to threat patterns and provide an automated response. The TNI urgently needs this technology to improve its early detection capabilities against complex cyber attacks. Moreover *Big Data Analytics* has demonstrated its effectiveness in identifying hidden threat patterns. Bouke (2024) propose an SMRD framework that integrates big data analytics to understand threats such as ransomware and DDoS. This framework provides systematic guidelines for effectively detecting, analyzing, and counteracting threats. The TNI can use this technology to monitor suspicious activity in military communication networks. Another technology that can be used is honeypot (Purwoko et al., 2023). Honeypots are designed to attract attacks from cyber actors with the aim of learning their tactics and methods. The use of honeypots allows the TNI to study cyber threat patterns, provide strategic insights, and increase the effectiveness of mitigation measures.

Cyber Resilience in a Military Environment

Cyber resilience (*Cyber Resilience*) is the ability of a system to survive, respond to, and recover from cyberattacks without losing its critical functions (Hugyik, 2020). Cyber resilience in the military includes the protection of all strategic infrastructure, which is the operational basis of defense. Military infrastructure supports military operations, including communications networks, data centers, military satellites, logistics transportation, energy facilities, and maritime infrastructure.

Potential targets of cyberattacks include military communications infrastructure, data centers, satellites, and logistics transportation. As explained Kristian et al., (2022), ransomware attacks can disrupt logistics and delivery of equipment and other equipment to the area of operation, thereby weakening defense capabilities. An attack on the TNI's communication network and logistics system can cause major disruptions in the coordination of military operations, delays in logistics deliveries, and reduced troop readiness on the ground. The TNI needs a real-time monitoring system as well as network redundancy to maintain operational continuity. Energy infrastructure is also a very important element. According to Fedotenko (2023), attacks on power plants or energy distribution networks could undermine military operations that rely heavily on electricity supplies. Meanwhile, military communications satellites are a strategic target in cyber warfare, as damage to satellites can disrupt troop navigation, surveillance, and coordination systems. In this situation, the TNI needs a cyber resilience strategy that involves proactive and defensive systems to prevent and mitigate attacks.

Case Study of Cyber Defense Strategy Implementation

An effective cyber defense strategy relies not only on advanced technology but also on policy integration, personnel training, and cross-sector collaboration. Several countries have shown success in implementing cyber defense strategies that can be a reference for the TNI in building a more resilient defense posture. The United States, for example, through the US Cyber Command (USCYBERCOM), has built an artificial intelligence (AI)-based early detection system to anticipate threats to critical infrastructure. The system is capable of analyzing large amounts of data in real-time to detect unusual threat patterns (Prieto, 2021). In addition, the United States established the Cyber Mission Force, a cyber offensive team, to conduct offensive operations against threat actors. Close collaboration with the private sector through programs such as the Enduring Security Framework, which allows for the proactive exchange of information about threats, supports the success of this strategy.

Russia is taking a unique approach to geopolitical conflict by integrating cyber operations and information warfare as part of a hybrid warfare strategy (Setiyono, 2023). During the invasion of Ukraine in 2022, Russia systematically launched cyberattacks to cripple Ukraine's military communications network, while an information warfare campaign was deployed to divide society through disinformation (Fedotenko, 2023). One method used was a Distributed Denial-of-Service (DDoS) attack, which crippled Ukraine's communications infrastructure for weeks, creating operational and social chaos. This approach shows how cyberattacks are not only a technical tool, but also include psychological elements that are integrated with geopolitical strategies. The study highlights the need for the integration of advanced technology with digital propaganda strategies to create dominance in cyberspace.

The lesson that can be learned is the need to prepare strategies that are not only defensive but also offensive, so that they are able to counter information manipulation and maintain stability in cyberspace.

Lithuania provides a great example of how national resilience can be strengthened with an integrated cybersecurity strategy. Lithuania has adopted a comprehensive approach that involves cross-sectoral collaboration between the government, the private sector, as well as civil society, as the country is often the target of Russian attacks (Anwarrudin et al., 2023). This strategy includes simulating cyberattacks involving the financial and energy sectors, the establishment of a National Cyber Resilience Center, and cyber literacy programs to increase public awareness. In addition, Lithuania emphasizes international cooperation with NATO members, including joint exercises to prepare the country for hybrid attacks (Anwarrudin et al., 2023). This approach shows how important it is to build collaboration between domestic forces and international collaboration to confront complex and ever-evolving cyber threats. Lithuania's strategy can be an inspiration in creating an adaptive, inclusive, and collaboration-based cybersecurity system.

South Korea implements a cyber defense strategy that leverages technology *Information and Communication Technology (ICT)*such as artificial intelligence (AI) and big data analytics to monitor cyber activities in real-time. To create more sophisticated threat detection tools and improve defenses against cyberattacks, private companies such as Samsung and LG are working with the country's governments (Diara, 2020). The development of a big data-based platform that is able to thoroughly analyze threat patterns and provide a quick response to cyber incidents is also part of this approach. In addition, South Korea regularly conducts cyber defense exercises that simulate threats coming from state and non-state actors. The exercise not only aims to improve the capabilities of military personnel, but also to enhance cooperation between the public and private sectors. South Korea's success in mitigating cyber threats from North Korea shows that cross-sector cooperation with the integration of advanced technologies can result in a flexible and resilient cyber defense system.

Estonia, which was the target of a significant cyberattack in 2007, has managed to build a resilient cyber infrastructure using new strategies and technological innovations. Since the attack, Estonia has strengthened its cyber defense system by taking an important step, namely the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), which serves as a training and research center for NATO member states, is one of the steps (Firman, 2018). Estonia also uses cloud-based digital backup technology to store government data abroad. This allows the operation to keep going even if an attack occurs. In addition, the country is building a digital citizenship system, or e-citizenship, which has excellent protection to safeguard citizens' personal information. Estonia also requires cyber training for government employees as part of efforts to improve their readiness to deal with cyber threats (CCDCOE, 2023). Estonia has made cyber defense an important part of its national strategy and continues to encourage research and development to improve long-term resilience. This strategy ensures the protection of digital infrastructure and makes Estonia a pioneer in building an innovative and adaptive global cybersecurity system.

3. RESEARCH METHODS

This study uses a qualitative method with a descriptive-analytical approach to explore the threat of cyber warfare to national defense as well as strategies that can be adopted by the TNI in building a cyber defense posture. The qualitative approach was chosen because it allows researchers to understand the complex dynamics of cyber warfare that is constantly evolving. In addition, the study also leverages case studies from different countries to provide comparative insights that are important for identifying relevant solutions for the TNI. According to Rehardiningtyas et al. (2022), this approach is well suited for analyzing challenges that are multidimensional, such as cyber threats. In addition, this research uses the information and communication technology (ICT) adaptation paradigm to support national stability through strengthening the cyber defense posture (Dalimunthe et al., 2023).

4. DISCUSSION

Analysis of Cyber Threats to National Defense

Cyber threats have developed into one of the main challenges in maintaining Indonesia's national defense. Data from the State Cyber and Cryptography Agency (BSSN) shows that in 2022, Indonesia was recorded to face 84.8 million cyberattacks, with 1.7 million of them targeting the defense sector. This figure shows significant vulnerability, especially given Indonesia's limited

cyber defense infrastructure and capacity compared to developed countries. Distributed Denial-of-Service (DDoS), ransomware, phishing attacks, and hacking of military communications infrastructure are some of the most frequently encountered types of threats. Disruption of satellite-based communication networks or logistics infrastructure can hamper regional surveillance, coordination, and the TNI's response to threats. An attack on a military communication network can cripple the TNI's ability to respond to threats quickly and in an organized manner, both in the context of national border defense, operations on land, sea, and air. With increasing reliance on technology, these attacks can undermine operational stability across strategic units. Technological advances such as the use of encrypted networks and anonymity tools, such as Tor and VPN, have improved the ability of actors to hide their identities, making tracking and prevention a major challenge for Indonesia's defense system.

Candra et al. (2021) stated that cyber threats to the military include strategic aspects and technical damage. In this case, cyber espionage allows state and non-state actors to steal sensitive information such as intelligence data and military operation plans. In addition, information manipulation through social media has become an effective tool to weaken the morale of troops and create public unrest, as a vivid example of cyber threats can be seen in the Russia-Ukraine conflict, where DDoS attacks crippled Ukraine's strategic communications and logistics, creating significant disruptions in military coordination (Setiyono, 2023).

Technology and Human Resources (HR) Gap

The TNI faces major challenges in building a resilient cyber defense system due to limited technology and human resources (HR). Based on research by Candra et al. (2021), technical training in the field of cybersecurity has not become a top priority in Indonesian military education. In comparison, South Korea has integrated cyber training into their military curriculum, allowing for better preparedness in the face of complex threats. Additionally, threats to critical infrastructure, such as power plants, logistics systems, and communication networks, can have a direct impact on the effectiveness of military operations. Jang et al. (2023) shows that damage to cyber assets can affect the physical combat capabilities of a military organization. This shows that the framework needed to evaluate the operational impact of cyberattacks is critical.

In addition, the TNI's technological infrastructure is not adequate to effectively manage cyber threats. For example, Indonesia does not yet have *Cyber Range Simulation*, which is a simulation-based training platform that allows personnel to test responses to cyber threats in controlled scenarios. Yamin et al. (2020) Suggest the use of advanced technologies such as Cyber Range, a simulation platform that allows training and testing of cybersecurity strategies. Countries such as Estonia have leveraged these simulations to engage strategic sectors, including energy and communications, thereby increasing readiness to face real threats. Cyber range strengthens the TNI's operational readiness by providing a secure environment to test responses to various threats, such as ransomware and DDoS attacks. The first step to building a cyber range simulation can begin by adapting the Estonian model that integrates cloud technology and cross-sector training. The TNI can work with BSSN to build these simulations through partnerships with local technology universities and domestic technology companies in developing realistic scenario-based threat simulations.

The HR gap includes not only the number of trained personnel, but also the quality of training provided. Today, cyber training in military environments tends to be generalist, without deep specialization in threat detection, network security, or real-time response to cyberattacks. Hasan (2022) noted that at least one special cyber team is needed for each TNI operational unit to be able to respond to threats 24/7, but in reality, the number of these teams is still very limited. Short-term solutions can be in the form of cybersecurity certification through training programs based on cooperation with technology universities such as ITB or the University of Indonesia. Meanwhile, the long-term solution includes the development of officers who graduated from specialized military academies in cyber security that produce expert personnel in this field.

Case studies from developed countries provide important insights into collaborative and innovative approaches to building cyber resilience. The following is a table that presents a comparison of cyber defense strength between Indonesia and several other countries:

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

https://ijpsat.org/
Vol. 48 No. 1 December 2024, pp. 451-461

Table 1. Comparison of Cyber Defense Forces Between Indonesia and Several Other Countries

Country	Policies and Regulations	Cyber Infrastructure	Technologies Used	International Collaboration	Key Advantages
United States	National Cyber Command Strategy (USCYBERCOM); Strict regulation	State-of-the-art infrastructure with large data centers	AI, big data analytics, offensive cyber operations	NATO, program Enduring Security Framework	Strong offensive capabilities and public-private sector coordination
Russia	Flexible approach in hybrid warfare	Decentralized infrastructure	Disinformation, DDoS attacks, and malware	Strategic partnerships with several Eastern European countries	Cyber integration with information warfare for geopolitical purposes
Lithuania	A collaborative national security framework	Centralized and integrated security system	AI, cyber simulation	NATO, Baltic regional cooperation	Cross-sector collaboration and cyber literacy programs
South Korea	National digital security policy	Modern infrastructure with integrated systems	AI, big data analytics	Technology partnerships with the private sector (Samsung, LG)	Integration of advanced technologies to mitigate threats from North Korea
Estonia	Digital-based security strategy	Backup cloud infrastructure	Blockchain, e-citizenship, honeypots	NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)	Leader in the adoption of cyber technology and digital security systems
Indonesia	BSSN as the main regulatory body	Infrastructure is evolving	Big data analytics (in development)	ASEAN, regional initiatives	Great potential but facing challenges of resources and technological readiness

Source: Results of Analysis processed by the author team, (2024).

From the table, the TNI needs to develop a more integrated strategy with the increasing frequency and complexity of cyberattacks. The TNI can learn from the US Cyber Command (USCYBERCOM) model, particularly in the formation of special units such as the Cyber Mission Force that focus on offensive and defensive responses. In addition, South Korea's collaboration with the private sector demonstrates the importance of local partnerships to accelerate the development of cybersecurity technologies relevant to national needs. Cooperation with ASEAN could include the establishment of a regional cyber threat data-sharing network, which utilizes AI systems to detect cross-border threats. These efforts not only protect the military's infrastructure but also ensure that the military is prepared to deal with evolving cyber threats around the world.

Innovation-Based Technology Strategy in TNI Defense System

To overcome existing limitations, the TNI needs to adopt innovative technologies that are able to improve the detection, mitigation, and response to cyber threats. The main challenges in the application of advanced technology are the readiness of infrastructure and the high initial investment costs. For example, the implementation of AI technology for cyber threat analytics requires secure and fast data centers, while blockchain requires a distributed network with high processing capacity. To overcome this obstacle, the TNI can adopt a gradual approach, starting with the integration of honeypots and *cyber deception tactics* as a more affordable first step. This technology not only provides temporary protection but also serves as an attack analysis laboratory to identify complex threat patterns. In addition to supporting technological innovation, local startup collaborations such as GoTo can help the TNI analyze data-driven threat patterns in real-time, while SIRCLO, can help build cloud-based communication solutions with high levels of encryption to support military operations, while Barantum offers a CRM system that enables more effective management of strategic information. In addition to being able to reduce dependence on foreign technology vendors, as well as supporting the development of the domestic technology ecosystem.

1. **Artificial Intelligence (AI):**

AI helps strengthen cyber defense capabilities because it can analyze data in real-time. This allows for early detection of hidden threat patterns. Zhao et al. (2022) shows that AI can be used to process big data effectively, improving speed and accuracy in detecting attacks. Security Orchestration, Automation, and Response (SOAR) is one of the relevant AI applications that enables automated response to threats with high efficiency (Gustina DM & Ananda, 2024). The use of AI in the TNI environment can provide a competitive advantage, especially in the face of sophisticated attacks such as AI-based malware.

2. **Big Data Analytics:**

Big data provides the analytical ability to process large amounts of information, helping to identify threat patterns and predict future attacks. SMRD Framework (*Social Engineering, Malware, Ransomware, Distributed Denial-of-Service*), developed by Bouke & Abdullah, (2024), is one example of how big data analytics can be used to understand and deal with complex cyber threats. The integration of big data in defense systems allows the TNI to make optimal use of operational data, improve threat detection, and strengthen response to cyber attacks.

3. **Blockchain:**

Blockchain is an innovative way to keep military data clean and transparent. Cha et al. (2020) creating a blockchain-based cyber threat intelligence system structure that enables more secure data collection and management. Military data and operational communications can be protected from leakage or manipulation with this technology. Additionally, blockchain can be used to share cyber threat information in a decentralized manner, helping cross-sectors work together to find and combat threats. Data security is a crucial aspect that needs to be considered in the adoption of blockchain technology, which not only maintains the integrity of military data but also prevents potential leakage of strategic information

4. **Honeypot and Cyber Deception Tactics:**

Honeypots are designed to prevent cyberattacks and identify threat patterns used by actors. Honeypots can be used to test defense strategies and find system weaknesses. By integrating *cyber deception tactics*, the TNI can divert the attention of threat actors to fake systems and utilize attack data to improve mitigation.

5. **Cyber Range Simulation:**

Cyber range-based simulations provide opportunities for the TNI to train response to threats in a controlled environment. Yamin et al. (2020) stated that this platform is essential to improve operational readiness. The TNI can consistently test and improve cybersecurity strategies through simulations that include ransomware and DDoS attacks.

Integration of Strategies and Collaboration in Facing Cyber Threats

To confront increasingly complex cyber threats, the TNI needs a multi-disciplinary approach that includes advanced technology, intensive training, and cross-sector collaboration. Sulich et al. (2021) emphasized that cooperation between the public sector, the private sector, and education is essential to build sustainable cyber resilience. For example, Samsung and LG, technology companies, are helping the South Korean government develop advanced cybersecurity technologies (Oh et al., 2024). Collaboration with local technology companies such as GoTO, Barantum, Sirclo, Moka can help the TNI in accelerating the development of AI-based and big data-based solutions tailored to military needs. For example, GoTo can provide a big data-based platform designed to detect attack patterns on military communication networks. Barantum can help build a custom CRM system that allows for quick coordination between military operational units. In addition, collaboration with the private sector can also include the development of *Cyber Defense Innovation Hub*, which acts as an integrated research and training center under the coordination of the TNI and BSSN. This step can accelerate the development of domestic technology, as well as increase the readiness of personnel. Collaboration can be initiated at the regional level with the establishment of *Cyber Defense Innovation Hub*, which serves as a platform to connect the TNI, BSSN, the private sector, and academics, through technology-based universities such as ITB or the University of Indonesia, which are focused on joint research and training of military personnel in the face of cyber threats.

At the regional level, Indonesia can strengthen cooperation with ASEAN to create a resilient cybersecurity alliance. This strategy will not only strengthen national resilience but also improve the TNI's capabilities in dealing with cross-border cyber threats. This collaborative approach ensures that the TNI can respond to threats quickly, effectively, and in an integrated manner. Awareness of cyber threats in society and institutions needs to be increased. Arbidane & Purii (2024) shows that integrated cybersecurity education programs in Europe have succeeded in making people more prepared for attacks. A similar method can be applied in Indonesia by incorporating cyber education into the government curriculum. To be prepared for ever-evolving cyber threats, the military needs specialized training and technical capability development (Nifakos et al., 2021).

With the increasing complexity of cyber threats, the TNI needs to immediately implement strategic measures, both through the adoption of advanced technology, human resource development, and cross-sector collaboration. This step will not only improve national cyber defense capabilities but also strengthen Indonesia's position as a resilient country in facing global threats in the digital era.

5. Conclusion

Cyber threats have developed into one of the main challenges for Indonesia's national defense, especially for the Indonesian National Army (TNI), which is responsible for the country's stability and security. With 1.7 million cyberattacks targeting the defense sector in 2022, threats such as Distributed Denial-of-Service (DDoS), ransomware, and cyber espionage continue to rise. This is exacerbated by the limitations of technological infrastructure, the lack of competent human resources (HR), and the weakness of cross-sector and international collaboration.

The study concludes that advanced technology-based approaches, human resource development, and strategic collaboration can be solutions to build a more resilient cyber defense posture. Some of the proposed flagship solutions include:

1. **Establishment of Cyber Rapid Response Unit (CRRU):**

   This specialized unit is designed to respond to cyberattacks quickly and coordinated. CRRUs can be trained using cyber range simulation platforms, which allow testing of defense strategies in real-world threat scenarios. To improve efficiency, these units can include specialized sub-units such as the Maritime Cyber Defense Task Force,

which focuses on protecting communication and logistics networks in strategic areas such as sea borders and islands.

2. **Virtual Reality (VR)-Based Simulation:**

   VR technology provides a new approach to cyber defense training, allowing personnel to practice in tactical simulations that are close to real conditions. By integrating cyber threats into military operational scenarios, these simulations can improve personnel readiness to deal with complex multidimensional threats.

3. **Honeypot and Cyber Deception Tactics Integration:**

   This strategy allows the TNI not only to defend but also thwart attacks in the early stages. Deceptive Threat Environments built through honeypots can distract attackers while providing valuable data on their attack patterns and strategies. This data can be used to strengthen cyber defense systems on an ongoing basis.

4. **Cross-Sectoral and International Strategic Collaborations:**

   The establishment of the Cyber Defense Innovation Hub, which involves the government, the private sector such as GoTo, SIRCLO, and Barantum, as well as academics, can accelerate the development of local technology-based solutions such as AI and blockchain. Collaboration with international organizations such as the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) can provide access to the latest technology, strategic training, and threat information exchange globally.

5. **Blockchain-Based Monitoring and Evaluation Framework:**

   Blockchain can be used to protect military data while also functioning as a real-time monitoring system to maintain transparency and integrity of threat data. The technology has been successfully implemented in the United States through a blockchain-based platform to monitor military parts and protect strategic communications with end-to-end security. With this integration, the TNI can strengthen data security, evaluate defense strategies and adapt them to the latest threats.

6. **Establishment of Offensive Cyber Operations Unit:**

   Adopt an offensive approach through the establishment of specialized cyber operations units designed to counterattack threat actors. This unit can carry out strategic operations such as digital information warfare, manipulation of enemy narratives, and destruction of the opponent's cyber network.

By implementing these solutions, the TNI can build a more resilient, innovative, and adaptive cyber defense against global threat dynamics. This approach not only protects the military's strategic infrastructure, but also creates a sustainable and inclusive national cybersecurity ecosystem. The successful implementation of these measures will make the TNI a pioneer in cyber defense in the Southeast Asian region, as well as strengthen Indonesia's position in facing global challenges in the digital era.

References

[1]. Anwarrudin, M., Sunarko, B. S., & Trihartono, A. (2023). *The Republic of Lithuania's Response to the Shadow of Russia's Fifth-Generation War Threat*.

[2]. Arbidane, I., & Purii, H. (2024). *IMPLEMENTATION OF INTEGRATED CYBER EDUCATION IN EUROPE. II*, 156–166.

[3]. Azzani, I. K., Adi Purwantoro, S., & Zakky Almubarok, H. (2024). Enhancing awareness of cyber crime: a crucial element in confronting the challenges of hybrid warfare in indonesia. *Defense and Security Studies,*.

[4]. Baloch, R. (2019). Cyber Warfare Trends, Tactics and Strategies: Lessons for Pakistan. *Journal of Development Policy, Research & Practice (JoDPRP), 3*(1), 23–43. https://doi.org/10.59926/jodprp.vol03/02

[5]. Bouke, M. A., & Abdullah, A. (2024). SMRD: A Novel Cyber Warfare Modeling Framework for Social Engineering, Malware, Ransomware, and Distributed Denial-of-Service Based on a System of Nonlinear Differential Equations. *Journal of Applied Artificial Intelligence*, *5*(1), 54–68. https://doi.org/10.48185/jaai.v5i1.972

[6]. Candra, A., Suhardi, S., & Persadha, P. D. (2021). Indonesia facing the threat of cyber warfare: a strategy analysis. *Defense Journal: Information Media TTG Studies &*

[7]. Cha, J., Singh, S. K., Pan, Y., & Park, J. H. (2020). Blockchain-based cyber threat intelligence system architecture for sustainable computing. *Sustainability (Switzerland)*, *12*(16), 1–18. https://doi.org/10.32890/JICT2018.17.3.8260

[8]. Dalimunthe, A. A., Suwito, S., & Asmoro, N. (2023). Strategy for Building an Ecosystem for the Maintenance of the Main Tools of the National Weapon System in the Face of Technological Developments. *JIIP - Scientific Journal of Educational Sciences*, *6*(6), 4192–4195. https://doi.org/10.54371/jiip.v6i6.1777

[9]. Diara, D. D. (2020). *SOUTH KOREA'S CYBERSECURITY STRATEGY.*

[10]. Fedotenko, A. (2023). *Cyber warfare as part of information warfare of Russia against Ukraine since the beginning of the 2022 Russian invasion. Věda a perspektivy. 8*(27), 351–357.

[11]. Firman, F. A. (2018). Estonia's cyber defense policy in responding to Russia's cyber sabotage to Estonia. *Indonesian Computer University*. https://elib.unikom.ac.id/files/disk1/799/jbptunikompp-gdl-fathikaanj-39937-4-unikom--i.pdf

[12]. Gustina DM, V., & Ananda, A. (2024). Artificial Intelligence for Security Orchestration, Automation and Response: A Scope Review. *Journal of Applied Computing*, *10*(1), 36–47. https://doi.org/10.35143/jkt.v10i1.6247

[13]. Honeynet, BSSN, 2022. (2022). *Honeynet Project BSSN Annual Report 2022 - IHP*. 1–85. https://cloud.bssn.go.id/s/qSJenLAmr2ooF2Q

[14]. Hugyik, A. (2020). Best practices in the application of the concept of resilience: building hybrid warfare and cybersecurity capabilities in the hungarian defense forces. *Connections*, *19*(4), 25–38. https://doi.org/10.11610/Connections.19.4.02

[15]. Jang, J., Kim, K., Yoon, S., Lee, S., Ahn, M., & Shin, D. (2023). Mission Impact Analysis by Measuring the Effect on Physical Combat Operations Associated With Cyber Asset Damage. *IEEE Access*, *11*(April), 45113–45128. https://doi.org/10.1109/ACCESS.2023.3273612

[16]. Kristian, I., Rochaeni, A., State, S. A., Studies, P., Government, I., General, U., & Yani, A. (2022). *Military strategy regarding cyber for cyber superiority in electronic warfare*. *6*(2), 207–216.

[17]. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2023). *Cybersecurity Practices for Military Organizations*. https://ccdcoe.org/

[18]. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). *Influence of Human Factors on Cyber Security within Healthcare Organisations : A Systematic Review*. 1–25.

[19]. Oh, S. J., Cho, S. K., & Seo, Y. (2024). Harnessing ICT-Enabled Warfare: A Comprehensive Review on South Korea's Military Meta Power. *IEEE Access*, *12*(April), 46379–46400. https://doi.org/10.1109/ACCESS.2024.3378735

[20]. Prieto, J. (2021). *The integration of AI in US Cyber Command's cybersecurity strategy. Journal of Defense Technology, 15(3), 205–217.*

[21]. Purwoko, R., Febriyan, D. P., Adhe, G. P., Laksito, W. S. Y., Siswanti, S., & Hasbi, M. (2023). Honeypot-as-a-Service with Kubernetes Cluster. *Jepin*, *9*(2), 204–2017.

[22]. Rehardiningtyas, D. A., Firdaus, M. F., & Sulistyanto, S. (2022). Military Leadership Competencies in the Society 5.0 Era. *Journal of Citizenship*, *19*(2), 126. https://doi.org/10.24114/jk.v19i2.35229

[23]. Setiyono, A. (2023). *THE DYNAMICS OF RUSSIA'S DEFENSE STRATEGY THROUGH HYBRID WARFARE IN THE CONFLICT WITH UKRAINE IN 2020 - 2023*.

[24]. Sholikah, D. I., Harbriyana Putra, T., & Fauzan Hidayat, M. (2024). Cyber Warfare Is The Newest Challenge To Support Indonesian National Resilience. *Asian Journal of Social and Humanities*, *2*(9), 2000–2006. https://doi.org/10.59888/ajosh.v2i9.332

[25]. Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and sustainable development. *Procedia Computer Science*, *192*(May), 20–28. https://doi.org/10.1016/j.procs.2021.08.003

[26]. Yamin, M. M., Katt, B., & Gkioulos, V. (2020). *Cyber ranges and security testbeds: Scenarios, functions, tools and architecture*. https://doi.org/10.1016/j.cose.2019.101636

[27]. Zhao, L., Zhu, D., Shafik, W., Matinkhah, S. M., Ahmad, Z., Sharif, L., & Craig, A. (2022). Artificial intelligence analysis in cyber domain: A review. *International Journal of Distributed Sensor Networks*, *18*(4). https://doi.org/10.1177/15501329221084882