East Asian Journal of Multidisciplinary Research (EAJMR)
Vol. 4, No. 3, 2025 : 987 - 1006

Enhancing Cyber Defense Capabilities through AI Technology

Septian Dhika Aditya[1]*, Achmad Farid Wadjdi[2], Danang Rimbawa[3]
Republic of Indonesian Defense University
Corresponding Author: Septian Dhika Aditya septian.dhika@tp.du.ac.id

A R T I C L E I N F O
Keywords: Cyber Defense, Artificial Intelligence, Technology

Received : 15 January
Revised : 06 February
Accepted: 08 March

A B S T R A C T
The development of cyber threats is impacting vital communications infrastructure, with a focus on 5G security, AI, and international cooperation. The purpose of this study is to analyze Enhancing Cyber Defense Capabilities through AI Technology. The research method used in this study is qualitative descriptive. The results of this study show that: First, the use of advanced AI technology in every aspect of the TNI will improve the overall security of the application. AI technology is able to detect and respond to cyber threats quickly and accurately, strengthening operational capabilities on land, sea, air, cyber, and space. Second, the integration of AI in the defense system through the Fourth Industrial Revolution will increase the efficiency and effectiveness of TNI operations in various dimensions. AI aids in the detection, analysis, and response to threats, strengthens decision-making capabilities in the field, and improves the combat readiness of troops. Third, the launch of STRANAS-KA is the foundation for the development of AI experts in the TNI, improving technical and managerial capabilities in AI to optimize the use of AI technology in defense operations. Finally, collaboration with the private sector enables the development of innovative AI solutions in defense operations, improves operational efficiency, and strengthens national resilience against increasingly complex and sophisticated cyber threats.

DOI : https://doi.org/10.55927/eajmr.v4i3.85
ISSN-E: 2828-1519
https://mtiformosapublisher.org/index.php/eajmr

INTRODUCTION

The cyber threat landscape has expanded with the growth of online channels, smartphones, and digital services. This has impacted national efforts to support vital communication infrastructure, especially mobile communication. In May 2022, the US introduced a 5G security evaluation process to strengthen cyber security standards for federal agencies. The hope is that mobile data infrastructure will accelerate the adoption of IoT and Industry 4.0 automation applications. South Korea is focusing on 5G security through collaborative efforts for future connectivity. Countries with low cyber security are also planning ambitiously, such as Spain's Digital 2025 program. Geopolitical instability is driving the national agenda to secure critical infrastructure. For example, Germany is enhancing SME resilience against cyber attacks. International cyber criminal activities have led to a series of ransomware attacks, such as on Italy's energy provider. Cyber security remains a top concern, as acknowledged by Aramco's CEO. In other words, cyber defense is crucial in protecting information systems and networks from cyber threats like hacker attacks and malware. These threats can jeopardize privacy, information security, and the economy. To address this, security technologies such as firewalls and antivirus software are important for blocking cyber attacks and conducting regular security audits. Education and awareness about cyber defense are also necessary (Ahn et al., 2021).

The government also plays a crucial role in ensuring effective cyber defense through regulations and technical support. Despite increasingly sophisticated cyber defense technologies, challenges such as system updates and lack of awareness about the importance of cyber defense remain issues. The use of artificial intelligence (AI) is a crucial solution in cyber defense. AI can help prevent and mitigate cyber threats with its ability to process data quickly and accurately. The Fourth Industrial Revolution, heavily reliant on AI, also presents significant potential in changing the dynamics of security and defense industries. The launch of Indonesia's National Artificial Intelligence Strategy (STRANAS-KA) demonstrates a serious commitment to implementing AI across various domains, yet the utilization of AI in national defense still needs further integration and expansion (Smith, 2022).

Artificial intelligence (AI) technology is the latest advancement with great potential to enhance productivity, accelerate innovation, and provide convenience for society. The use of AI has brought significant financial benefits in various fields, such as transportation and healthcare. In the context of national defense, cyber defense is highly crucial due to the complex cyber threats arising from technological advancements. The use of AI in cyber defense provides an advantage in military prevention actions. AI can train systems to recognize broader and dynamic attack patterns, providing effective defense against cyber attacks (Sutton, 2018).

Cyber security threats can originate from various sources and have diverse impacts. AI can be used to better support cyber operations and security compared to traditional strategies solely reliant on human intelligence in the virtual world. The utilization of AI technology in cyber defense is crucial to

keep pace with technological developments and address increasingly complex cyber threats. AI implementation can provide more adaptive and dynamic defense against cyber attacks, thereby enhancing the security of national information systems and networks (Latour, 2005).

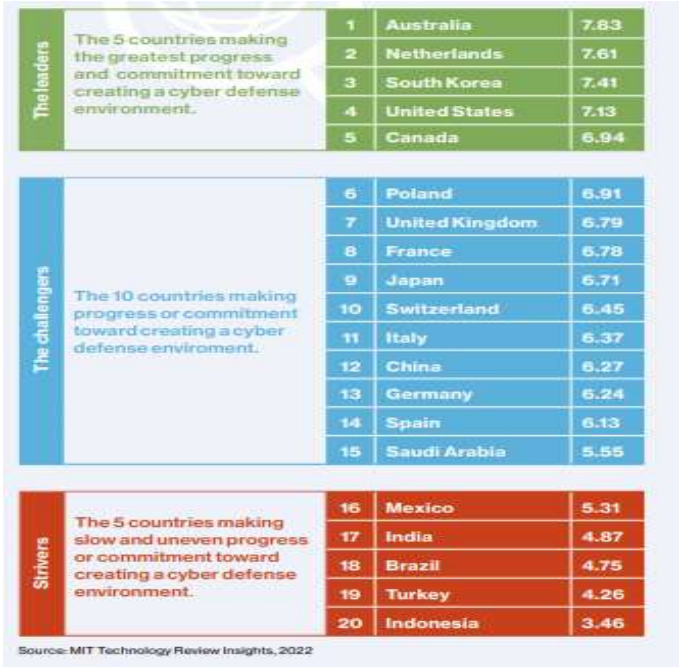

Figure 1. Cyber Defense Index Country

Source : MIT Technology Review, 2022

In the context of cybersecurity, critical infrastructure encompasses IT and communication networks that drive the digital economy. The top countries in this index include Australia, the Netherlands, and South Korea. Their primary focus is strengthening digital infrastructure to maintain essential cybersecurity and resilience crucial for societal productivity. Meanwhile, Indonesia is one of the five countries showing slow and uneven progress in building a cyber defense environment. The pillars in building cyber defense as referred to in the Cyber Defense Index are Pillar 1: Critical Infrastructure measuring the capacity and security of information and communication technology infrastructure (30% CDI score). Pillar 2: Cyber Security Resources assesses technology and law enforcement for cybersecurity assets (35%). Pillar 3: Organizational Capacity evaluates digital business maturity and experience (20%). Pillar 4: Policy Commitment assesses the effectiveness and quality of government cybersecurity regulations (15%). Therefore, Indonesia must build capabilities in the field of national defense using AI (MIT Technology Review, 2022).

LITERATURE REVIEW

Cyber Defense Theory

Cyber defence theory revolves around the strategies and methodologies employed to protect information systems and networks from cyber threats and attacks. It encompasses various aspects such as prevention, detection, response,

and recovery to ensure the integrity, confidentiality, and availability of data. One key aspect of cyber defence is the implementation of multi-layered security measures, also known as defence-in-depth. This approach involves deploying multiple security controls at different layers of the IT infrastructure to create a robust security posture (Gollmann, 2011). Techniques include firewalls, intrusion detection systems (IDS), encryption, and secure access controls.

Another crucial element is threat intelligence, which involves gathering and analysing data on potential and emerging cyber threats. This intelligence helps organisations proactively identify vulnerabilities and take preemptive actions to mitigate risks (Choo, 2011). Incident response is also a critical component of cyber defence. This involves having a well-defined plan and team in place to respond to security breaches promptly, minimizing damage, and restoring normal operations (Whitman & Mattord, 2013). Moreover, continuous monitoring and regular security assessments are vital for maintaining an effective cyber defence strategy. These practices ensure that security measures are up-to-date and capable of defending against the latest threats (Tipton & Krause, 2012). In conclusion, cyber defence theory integrates various practices and technologies aimed at safeguarding information systems from cyber threats, emphasizing prevention, real-time monitoring, and responsive actions.

Artificial Intelligence Theory

Artificial Intelligence (AI) theory focuses on the development of systems capable of performing tasks that typically require human intelligence. These tasks include reasoning, learning, problem-solving, perception, and language understanding (Russell & Norvig, 2016). One of the foundational theories in AI is the concept of machine learning, which enables systems to learn from data and improve their performance over time without being explicitly programmed. Supervised learning, unsupervised learning, and reinforcement learning are primary methodologies within this domain (Mitchell, 1997). Supervised learning involves training a model on a labelled dataset, whereas unsupervised learning finds patterns in unlabelled data. Reinforcement learning uses a system of rewards and penalties to train algorithms based on trial and error (Sutton & Barto, 2018).

Another critical aspect of AI theory is natural language processing (NLP), which enables machines to understand and interpret human language. Techniques in NLP involve syntax, semantics, and context analysis to achieve meaningful interactions between humans and machines (Jurafsky & Martin, 2008). The theory of neural networks, inspired by the human brain, is also central to AI. These networks consist of interconnected nodes (neurons) that process information in layers, allowing for complex pattern recognition and decision-making tasks (Goodfellow et al., 2016). In conclusion, AI theory encompasses a range of methodologies and concepts aimed at creating intelligent systems. These include machine learning, natural language processing, and neural networks, each contributing to the broader goal of mimicking human cognitive functions.

Technology

The theory of technology explores how technological advancements shape, and are shaped by, society, economy, and culture. It examines the interplay between technological development and human activity, considering both the positive impacts and potential drawbacks. One prominent framework within this theory is the Social Construction of Technology (SCOT). SCOT posits that technology is not an autonomous force but is shaped by social, economic, and political factors. According to this perspective, various social groups influence the development and acceptance of technological innovations based on their interests and power dynamics (Bijker, Hughes, & Pinch, 1987).

Technological Determinism, another critical theory, argues that technological innovation is the primary driver of societal changes. Proponents believe that technology evolves according to its own logic and significantly influences social structures and cultural values (Smith & Marx, 1994). Actor-Network Theory (ANT), developed by Bruno Latour and others, examines the network of relationships between human and non-human actors involved in the creation and use of technology. ANT emphasises that both social and technical elements are intertwined and co-evolve, suggesting that technological artefacts and human actors collectively shape technological outcomes (Latour, 2005). In conclusion, the theory of technology encompasses various perspectives, including SCOT, Technological Determinism, and ANT. These frameworks provide insights into how technology develops and its profound effects on society and human behaviour.

METHODOLOGY

This research is descriptive with a qualitative approach, where initially the author explained about space diplomacy. After that, the author discussed the perspective Enhancing Cyber Defense Capabilities through AI Technology. Furthermore, the author describes every subtheme about space diplomacy.

The research methods used are literature study and secondary data analysis. Data is taken from various sources in the form of library materials, consisting of previous research, scientific journals, books, government reports, official news, and information from trusted and relevant websites related to the Enhancing Cyber Defense Capabilities through AI Technology.

Data analysis techniques use theories from Milles, Huberman and Saldana (2014), namely data collection, data condensation, presenting data (data display), and drawing conclusions or verification (conclusion drawing and verification). The validity test of the data used is Credibility (Internal Validity), Transferability (External Validity), Dependability (Reliability) and Confirmability (Objectivity) carried out at each stage it is described in the following research design:

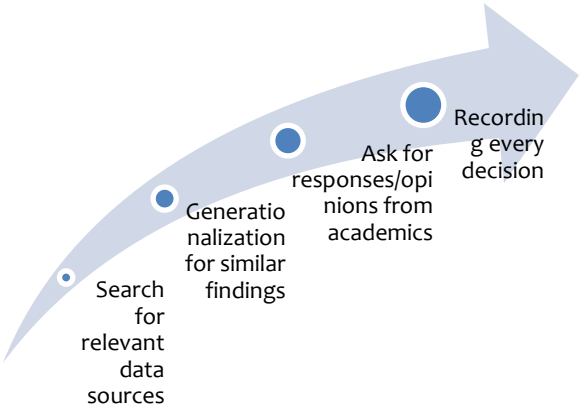

Figure 2. Research Design
Source : Processed by the author, 2024

RESEARCH RESULT AND DISCUSSION

The use of artificial intelligence (AI) in cyber defense is becoming increasingly important given the ever-evolving threats, especially cyberwarfare that is increasingly rampant. Attacks on government websites such as the KPU and the Directorate General of Taxes show the vulnerability of our systems to digital attacks. One of the major threats is ransomware, social engineering, and malicious insider activity. Even Bank Indonesia was once the target of the Conti ransomware attack, which encrypted some of their data. Another phenomenon that is starting to emerge is the virtual art market using cryptocurrencies, which needs to be monitored by law enforcement agencies to prevent money laundering crimes (Dua et al., 2018).

In facing this threat, the Indonesian government and people need to understand and utilize technology effectively. One way is to use artificial intelligence (AI) in cyber defense. AI can be used for attack detection by monitoring abnormal network activity patterns and analyzing data quickly. Additionally, AI can be used for behavioral analysis to identify human attacks such as phishing. By utilizing machine learning algorithms, AI can learn repetitive attack patterns and distinguish between normal and unusual activity (Khattak et al., 2020).

AI can also improve application security by detecting weaknesses and fixing security issues before they are exploited by attackers. This includes user authentication, detection of attacks such as SQL and DDoS injections, and log analysis to detect suspicious activity. The application of AI in cyber defense not only improves detection and response to attacks, but also helps in understanding complex attack patterns and preventing greater losses. However, it is important to pay attention to the weaknesses and limitations of AI and ensure that the use of AI is in accordance with applicable regulations to protect data privacy and security (Mahmood et al., 2019).

The use of artificial intelligence (AI) in cyber defense is becoming increasingly important in today's era, where cyber threats are increasingly complex and serious. Threats such as hacker attacks, malware, data theft, and other cyberattacks can result in huge losses for individuals, companies, and countries. AI has the ability to process and analyze large amounts of data

quickly and accurately, making it particularly useful in preventing and addressing cyberattacks (Frigge et al., 2019).

AI can be used in several key areas in cyber defense (Sicker et al., 2018):

1. **Attack Detection:** AI can monitor network activity and recognize abnormal patterns that may be signs of an attack. This makes it possible to warn network administrators and block attacks before they damage the system.
2. **Comportamental Analytics:** AI can learn and analyze normal behavior patterns from users and applications, so it can warn if there are any suspicious changes. This helps prevent attacks such as phishing that involve human interaction.
3. **Improve Application Security:** AI can help find weaknesses in applications and fix security issues before they are exploited by attackers. By monitoring and analyzing application activity, AI can detect potential attacks and threats, as well as assist in obtaining quick and effective responses and defensive actions.

In the context of cyber defense, it's important to remember that while AI has many benefits, it also has its drawbacks and limitations. For example, accuracy issues and errors in pattern recognition can affect the effectiveness of AI in detecting attacks. Therefore, it is necessary to implement AI as part of a holistic cyber defense strategy, and set appropriately to ensure data privacy and security.

Table 1. SWOT Enhancing Cyber Defense Capabilities through AI Technology

STRENGTH	OPPORTUNITIES
• Advanced AI Technology: AI's ability to process data quickly and accurately provides an advantage in detecting and responding to cyberattacks effectively. • Fourth Industrial Revolution: The use of AI as part of the Fourth Industrial Revolution has great potential to change the dynamics of the security and defense industry. • STRANAS-KA: The launch of Indonesia's National Artificial Intelligence Strategy shows the country's seriousness in applying AI in various domains, including defense. • Increased Productivity: The use of AI in defense can increase productivity in detecting, analyzing, and responding to cyberattacks more quickly and efficiently. • Collaboration Between Government and Industry: Cooperation between government, industry, academia, and other institutions in the development of AI technology for defense provides synergy and access to the necessary resources.	• Improved Application Security: AI can help in the detection of weaknesses and threats in applications, thereby improving the overall security of the system. • Integration of AI in Defense: An opportunity to further integrate AI in a nation's defense system to confront increasingly complex threats in the digital age. • Expert Development: An opportunity to develop reliable experts in managing and optimizing AI technology for defense purposes. • Collaboration with the Private Sector: Closer cooperation with the private sector in the development of AI technology for national defense. • Strengthening IT Infrastructure:

	Efforts to strengthen the national IT infrastructure, including the use of own servers for the benefit of national defense
WEAKNESS	**THREATS**
• AI Accuracy Issues: Concerns about accuracy and errors in pattern recognition by AI can affect its effectiveness in detecting cyber attacks. • Utilization Limitations: Despite the great potential, the use of AI in cyber defense in Indonesia is still in the development stage and is not fully optimal. • Vulnerable IT infrastructure: The majority of IT infrastructure still relies on external servers, increasing vulnerability to cyberattacks that take advantage of system weaknesses. • Reliance on Technology: Excessive reliance on AI technology can become a vulnerability if the system is disrupted or hacked by irresponsible parties. • Difficulties in Expert Development: Further efforts are needed in the development of experts who are able to manage and optimize AI technology for the benefit of national defense.	• Ransomware and Malware Attacks: The threat of ransomware attacks, malware, and other types of cyberattacks that can result in significant losses to information systems and networks. • Fake Content: The potential for the spread of false information uses AI as a tool to spread disinformation and manipulate public opinion. • Over-Dependence: Over-reliance on AI technology in defense can be an opening for attackers to exploit system weaknesses. • Vulnerability to Intelligence Attacks: The use of AI in data collection and analysis can also increase vulnerability to intelligence attacks that use technology to hack and manipulate information. • Military Robotics Market: Advancements in AI technology can also accelerate the development of military robotics, which has a long-term impact on the balance of power and defense strategies.

Source : Data Processed by Researchers, 2024

Furthermore, in this SWOT analysis, performance identification is carried out through the **IFAS *(Internal Factor Analysis Summary)* analysis and EFAS *(External Factor Analysis Summary) analysis stages***, as follows:

Table 2. Internal Matrix of Analysis Factors Summary/ IFAS

IFAS		**WEIGHT**	**RATING**	**SCORE**	**KET**
Strength					
S.1	Advanced AI Technology: AI's ability to process data quickly and accurately provides an advantage in detecting and responding to cyberattacks effectively.	0,12	9	1,08	
S.2	Fourth Industrial Revolution: The use of AI as part of the Fourth Industrial Revolution has great potential to change the dynamics of the security and defense industry.	0,1	9	0,9	
S.3	STRANAS-KA: The launch of Indonesia's National Artificial Intelligence Strategy shows the country's seriousness in applying	0,11	7	0,77	

	AI in various domains, including defense.				
S.4	Increased Productivity: The use of AI in defense can increase productivity in detecting, analyzing, and responding to cyberattacks more quickly and efficiently.	0,07	8	0,56	
S.5	Collaboration Between Government and Industry: Cooperation between government, industry, academia, and other institutions in the development of AI technology for defense provides synergy and access to the necessary resources.	0,6	7	4,2	
Sub Total Strength		**1,00**		**7,51**	
Weakness					
W.1	AI Accuracy Issues: Concerns about accuracy and errors in pattern recognition by AI can affect its effectiveness in detecting cyber attacks.	0,13	1	0,13	
W.2	Utilization Limitations: Despite the great potential, the use of AI in cyber defense in Indonesia is still in the development stage and is not fully optimal.	0,2	2	0,4	
W.3	Vulnerable IT infrastructure: The majority of IT infrastructure still relies on external servers, increasing vulnerability to cyberattacks that take advantage of system weaknesses.	0,19	1	0,19	
W.4	Reliance on Technology: Excessive reliance on AI technology can become a vulnerability if the system is disrupted or hacked by irresponsible parties.	0,15	3	0,45	
W.5	Difficulties in Expert Development: Further efforts are needed in the development of experts who are able to manage and optimize AI technology for the benefit of national defense.	0,33	4	1,32	
Sub total Weakness		**1**		**2,49**	
Total		**2**		**10,00**	
Sub total Strength Difference – Sub total Weakness = 7.51-2.49 = (5.02)					

Table 3. External Factor Analysis Summary/ Efas Matrix

EFAS		WEIGHT	RATING	SCORE	KET
Opportunity					
0.1	Improved Application Security: AI can help in the detection of weaknesses and threats in applications, thereby improving the overall security of the system.	0,2	9	1,8	
0.2	Integration of AI in Defense: An opportunity to further integrate AI in a nation's defense system to confront increasingly complex threats in the digital age.	0,1	9	0,9	

0.3	Expert Development: An opportunity to develop reliable experts in managing and optimizing AI technology for defense purposes.	0,16	7	1,12	
0.4	Collaboration with the Private Sector: Closer cooperation with the private sector in the development of AI technology for national defense.	0,21	5	1,05	
0.5	Strengthening IT Infrastructure: Efforts to strengthen the national IT infrastructure, including the use of own servers for the benefit of national defense.	0,33	9	2,97	
Sub Total Opportunities		**1**		**7,84**	
Threats					
T.1	Ransomware and Malware Attacks: The threat of ransomware attacks, malware, and other types of cyberattacks that can result in significant losses to information systems and networks.	0,11	3	0,33	
T.2	Fake Content: The potential for the spread of false information uses AI as a tool to spread disinformation and manipulate public opinion.	0,09	5	0,45	
T.3	Over-Dependence: Over-reliance on AI technology in defense can be an opening for attackers to exploit system weaknesses.	0,16	3	0,48	
Q.4	Vulnerability to Intelligence Attacks: The use of AI in data collection and analysis can also increase vulnerability to intelligence attacks that use technology to hack and manipulate information.	0,31	5	1,55	
T.5	Military Robotics Market: Advancements in AI technology can also accelerate the development of military robotics, which has a long-term impact on the balance of power and defense strategies.	0,33	7	2,31	
Sub total Challenge		**1**		**5,12**	
Total		**2**		**12,96**	
Difference Sub total Opportunity – Sub total Challenge = 7.84 – 5.12 = (2.72)					

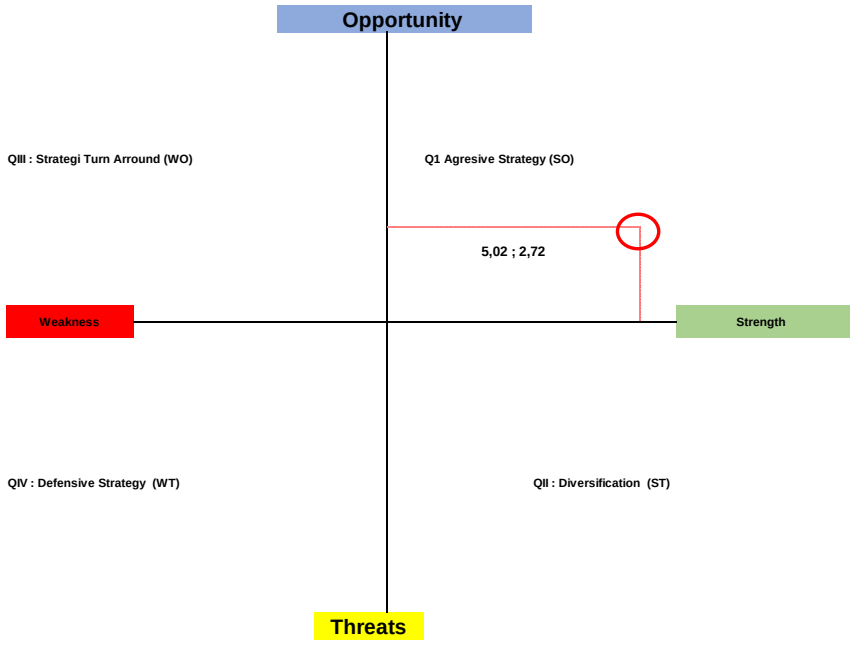

Figure 3. SO Strategy Enhancing Cyber Defense Capabilities through AI Technology

Source : Data Processed by Researchers, 2024

Based on the graph above, the Strength Opportunity or SO strategy is obtained which means:

1. Leveraging Advanced AI Technology for Improved Application Security

In an effort to improve application security, the use of advanced artificial intelligence (AI) technology is one of the main strategies. Advanced AI technology is able to detect and respond to threats to applications quickly and accurately, thereby improving overall system security and reducing the risk of cyberattacks. The implementation of this technology can be done by integrating AI systems into security software used by defense agencies. This ensures more effective early detection and mitigation of threats, which is crucial in the context of modern defense (Bennet et al., 2020). In the context of the TNI, the application of advanced AI technology can be integrated into various defense dimensions, namely the land dimension, the sea dimension, the air dimension, the cyber dimension, and the space dimension. Each dimension has special needs that can be met by utilizing AI.

Land Matra

For the ground dimension, AI technology can be used to improve the security of applications that manage intelligence, logistics, and operational data. AI can help detect cyber threats that try to access sensitive data or disrupt communication and command systems. Additionally, AI can be used in surveillance systems that utilize sensors and cameras to detect suspicious movements or threats on the battlefield. With fast and accurate analysis capabilities, AI helps accelerate decision-making in the field (UNIDIR, 2020).

Sea Matra

At sea, AI technology can be used in warship fleet navigation and management systems. Advanced AI systems can detect cyber threats that try to disrupt navigation or access the ship's control system. In addition, AI can be used in maritime surveillance systems to detect foreign vessels or suspicious objects in Indonesian waters. The implementation of AI in the ocean also includes the use of AI-equipped marine drones to conduct automated patrols and collect maritime intelligence data (Bennet et al., 2020).

Air Matra

In the air dimension, AI technology plays an important role in improving the security of applications used in the management of fighter aircraft and UAVs (Unmanned Aerial Vehicles) fleets. AI can help detect and respond to cyber threats that try to access flight control systems or disrupt communications between aircraft and bases. Additionally, AI can be used in air defense systems to detect and track enemy aircraft or suspicious flying objects. With its rapid analysis capabilities, AI helps improve the effectiveness of air operations and aviation safety (Bennet et al., 2020).

Cyber Matra

Cyber matra is the most directly related dimension to the use of AI technology to improve application security. AI can be used to detect cyberattacks, such as malware, phishing, and DDoS (Distributed Denial of Service), in real-time. AI systems can analyze attack patterns and provide automated responses to mitigate the impact of attacks before they damage the system. Additionally, AI can aid in cyber forensics to identify sources of attacks and strengthen overall cyber defenses (Bennet et al., 2020).

Space Matra

In space, AI technology can be used to improve the security of applications that manage satellites and space communication systems. AI can detect cyber threats that try to access satellite data or interfere with space communications. Additionally, AI can be used in space monitoring systems to detect alien objects or threats in space. The implementation of AI in the space dimension also includes the use of AI technology to analyze data collected by satellites and provide accurate and relevant information for defense purposes (Bennet et al., 2020).

By utilizing advanced AI technology in every aspect of the TNI, Indonesia's defense can improve its overall security. AI not only helps in detecting and responding to cyber threats quickly and accurately, but also strengthens operational capabilities on land, sea, air, cyber, and space. The integration of AI technology into defense systems allows the TNI to operate more efficiently and effectively in the face of various increasingly complex threats in this digital era.

2. Integration of AI in Defense Systems through the Fourth Industrial Revolution

The integration of artificial intelligence (AI) in defense systems through the Fourth Industrial Revolution (Industry 4.0) is a crucial strategic step in changing the dynamics of the security and defense industry. By incorporating AI as a core component of the Fourth Industrial Revolution, the defense industry can adapt quickly to increasingly complex and dynamic digital threats. This strategy not only improves operational efficiency but also strengthens the ability to detect, analyze, and respond to various security threats. The implementation of AI solutions covers various aspects of defense, from surveillance systems to intelligence data analysis, all of which aim to improve overall defense preparedness and response (Christensen, 2020).

Land Matra

At the ground level, the integration of AI in defense systems can be applied in various aspects, including surveillance, navigation, and intelligence data analysis. AI technology enables real-time analysis of data collected from various sensors in the field, so it can provide accurate and relevant information for military commanders. For example, drones equipped with AI can be used to monitor enemy movements and provide visual data directly to command centers, allowing for quick and timely decision-making. In addition, AI can be used in logistics management systems to optimize the distribution of resources and equipment on the battlefield, thereby improving the operational efficiency and combat readiness of ground forces (Allen, 2017).

Sea Matra

For the marine dimension, AI technology can be applied in the navigation and management systems of warship fleets. AI allows warships to operate more advanced and safe navigation systems, reducing the risk of human error and improving navigation safety. Additionally, AI can be used to analyze sonar and radar data in real-time, helping to detect underwater threats such as enemy submarines or sea mines. In the context of maritime surveillance, marine drones equipped with AI can conduct automated patrols and collect maritime intelligence data, which is then analyzed to detect suspicious activity or potential threats in Indonesian waters (Huang, 2019).

Air Matra

In the air dimension, the integration of AI allows for significant improvements in surveillance and air defense systems. AI-equipped fighter aircraft and UAVs (Unmanned Aerial Vehicles) can carry out surveillance and reconnaissance missions with higher efficiency. AI can analyze data from flight sensors to detect airborne threats such as approaching enemy aircraft or missiles, as well as provide tactical recommendations to UAV pilots or operators. Additionally, AI can be used in air fleet management systems to plan and optimize flight missions, reduce operational costs, and improve combat effectiveness (Roff, 2019).

Cyber Matra

In cyberspace, AI plays a very important role in detecting and responding to cyber threats. AI can be used to monitor network activity and detect cyberattack patterns in real-time, enabling a quick and effective response to emerging threats. AI systems can also be used to analyze forensic data after an attack has occurred, helping to identify attackers and strengthen future cyber defenses. Additionally, AI can be used in the development of more adaptive and proactive cybersecurity strategies, ensuring that cyber defense systems are always ready to face evolving threats (Taddeo, 2019).

Space Matra

In space, AI technology can be used to manage and operate satellites and space communication systems. AI allows the analysis of data from satellite sensors to detect threats in space, such as space debris or enemy satellite activity. Additionally, AI can be used to optimize satellite orbital paths and ensure secure and stable space communications. The implementation of AI in the space dimension also includes the use of AI technology to analyze data collected by satellites, providing accurate and relevant information for national defense and security purposes (Weeden, 2019).

By integrating AI in every dimension of defense through the Fourth Industrial Revolution, the TNI can significantly increase its operational efficiency and effectiveness. AI technology not only aids in the detection and response to threats, but also strengthens data analysis and decision-making capabilities in various situations. Thus, the integration of AI in defense systems is an essential strategic step to face security challenges in this digital era.

3. Launch of STRANAS-KA as the Basis for Expert Development in the Field of AI

The launch of the Indonesian National Artificial Intelligence Strategy (STRANAS-KA) is a strategic step that aims to develop experts in the field of artificial intelligence (AI) who are reliable and competent in managing AI technology in the defense sector. This strategy aims to harness the great potential of AI in improving Indonesia's overall defense capabilities. One of the important aspects of STRANAS-KA is the enhancement of special education and training programs for defense personnel, which focuses on developing technical and managerial capabilities in the field of AI. The implementation of this strategy involves improving the quality of military education as well as advanced training specific to AI, so that defense personnel can be better prepared to face future technological challenges (Indonesian Ministry of Research and Technology, 2020).

Land Matra

On the ground level, STRANAS-KA will encourage the development of AI experts who can optimize the use of advanced technology in ground operations. Military personnel will be trained to use AI in a variety of applications, such as intelligence data analysis, battlefield surveillance, and logistics management. With this expertise, the Army can improve the

effectiveness of combat operations and decision-making in the field. For example, AI algorithms can be used to analyze data from drones and sensors to detect the movement of enemies and other threats in real-time, allowing for faster and more accurate responses (Allen, 2017).

Sea Matra

For the maritime dimension, STRANAS-KA will strengthen the Navy's ability to use AI for maritime surveillance and underwater operations. The training program will include the use of AI in sonar and radar data analysis, automated navigation, and warship fleet management. Experts trained in AI will be able to develop and operate systems capable of detecting enemy submarines and other maritime threats more effectively. Additionally, AI can be used in fleet management to plan patrol missions and rescue operations, improving the efficiency and safety of maritime operations (Roff, 2019).

Air Matra

In the air dimension, STRANAS-KA will facilitate the development of AI experts for the Indonesian Air Force. The education and training program will focus on the application of AI in aerial surveillance, navigation, and aviation intelligence data analysis. AI technology can be used to monitor airspace, detect enemy aircraft, and manage air combat operations. For example, drones equipped with AI can perform reconnaissance missions more efficiently, while AI algorithms can assist pilots in tactical decision-making during combat operations (Huang, 2019).

Cyber Matra

In the cyber dimension, STRANAS-KA will play a key role in developing AI experts who can strengthen Indonesia's cyber defense. The training program will include the use of AI to detect and respond to cyberattacks, forensic data analysis, and the development of adaptive cybersecurity strategies. With this expertise, cyber defense personnel can be better prepared to face the ever-evolving threats in cyberspace. AI can also be used to monitor network activity and detect cyberattack patterns in real-time, allowing for a faster and more effective response to emerging threats (Huang, 2019).

Space Matra

In the space dimension, STRANAS-KA will encourage the development of AI experts who can manage and operate space technology more effectively. The education and training program will include the use of AI in satellite management, space data analysis, and space navigation. AI can be used to optimize satellite orbital paths and ensure safe and stable space communications. In addition, AI experts will be able to develop systems capable of detecting threats in space, such as space debris or enemy satellite activity, as well as providing accurate information for national defense and security purposes (Huang, 2019).

With the implementation of STRANAS-KA, TNI in every dimension will get AI experts who are trained and ready to face future technological challenges.

Education and training programs that focus on technical and managerial capabilities in AI will ensure that Indonesian defense personnel can optimize the use of AI technology in various defense operations, improving overall national defense preparedness and effectiveness.

4. Increasing Defense Productivity through Collaboration with the Private Sector

Increasing defense productivity through collaboration with the private sector is an important strategy to optimize the use of artificial intelligence (AI) in the detection, analysis, and response to cyberattacks. By partnering with leading technology companies, the defense sector can develop and implement innovative and advanced AI solutions in their operations. This strategy not only improves operational efficiency but also strengthens national resilience to increasingly complex and sophisticated threats (Ministry of Defense, 2020).

Land Matra

In the context of the Army, collaboration with the private sector allows the development of AI systems for battlefield surveillance and real-time threat detection. For example, tech companies can help develop advanced sensors and AI algorithms capable of analyzing data from various sources, such as drones and surveillance cameras, to detect enemy movements and other anomalies. This allows ground forces to respond to threats more quickly and precisely, increasing the effectiveness of combat operations. Additionally, AI can be used for more efficient logistics management, ensuring that the supplies and equipment needed are always available and accessible quickly (Stone, 2016).

Sea Matra

For the Navy, partnerships with technology companies can lead to the development of AI systems capable of optimizing maritime operations. AI can be used for sonar and radar data analysis, detecting enemy submarines, and monitoring ship movements in Indonesian waters. The collaboration can also produce automated navigation technology for warships, which improves the efficiency of maritime patrols and rescue operations. Additionally, AI can assist in fleet management and mission planning, ensuring that each ship operates at optimal efficiency and is prepared for a variety of threat scenarios (Goodman, 2007).

Air Matra

In the Indonesian Air Force, collaboration with the private sector can accelerate the development of AI technology for air surveillance and aviation intelligence data analysis. Technology companies can assist in creating systems capable of continuously monitoring airspace, detecting threats such as enemy aircraft or unidentified drones, and providing real-time information to pilots and central command. This technology not only improves preparedness and response to threats, but also provides a strategic advantage in air operations. Additionally, AI can be used for smarter and more efficient mission planning,

ensuring that each air mission can reach its destination with minimal risk (Franke, 2017).

Cyber Matra

In cyberspace, collaboration with the private sector is key to developing AI systems that are able to detect and respond to cyberattacks quickly and effectively. Tech companies have the expertise and resources to create AI solutions that can monitor network activity, detect cyberattack patterns, and perform forensic analysis to identify threat sources. The partnership also allows for the exchange of knowledge and technology, which can strengthen the TNI's overall cyber defense capacity. With advanced AI solutions, the TNI can ensure that critical infrastructure and sensitive data remain safe from evolving cyber threats (Franke, 2017).

Space Matra

For the space dimension, collaboration with the private sector can encourage the development of AI technology that is able to manage space operations more effectively. AI can be used for satellite management, including determining optimal orbital paths and detecting threats in space, such as space debris or enemy satellite activity. With the help of technology companies, the Indonesian Space Force can ensure that every space mission runs smoothly and safely, and is able to provide accurate data and information for the benefit of national defense. AI technology can also be used for more efficient and secure space communication, ensuring that all data sent and received is protected from potential threats (Franke, 2017).

By optimizing the use of AI through collaboration with the private sector, the TNI can increase productivity and operational effectiveness at all levels. This partnership allows access to cutting-edge technology and expertise needed to deal with future threats, as well as ensuring that Indonesia remains at the forefront of defense innovation.

5. Strengthening National IT Infrastructure to Support the Use of AI in Defense

Strengthening the national IT infrastructure to support the use of artificial intelligence (AI) in defense is an essential strategic step to ensure data security and system integrity in the face of increasingly complex threats. In this context, strengthening IT infrastructure, including the use of local servers for national defense purposes, is an important step that can support the implementation of AI in various military dimensions, namely the land, sea, air, cyber, and space dimensions (DARPA, 2019).

Land Matra

In the Army, strengthening the national IT infrastructure allows for the integration of AI systems that are more reliable and secure for field operations. Powerful and secure local servers ensure that data generated from various sensors, such as surveillance drones and surveillance devices, can be processed quickly and securely without the risk of external interference. Reliable IT

infrastructure also allows for more sophisticated data analysis for tactical decision-making on the battlefield, such as determining enemy positions or planning troop movements. In addition, the use of local servers reduces reliance on global networks that are vulnerable to cyberattacks, thereby increasing operational resilience (Goodman, 2007).

Sea Matra

For the Indonesian Navy, strengthening the national IT infrastructure allows for more effective and secure maritime data management. AI systems integrated with local servers can be used to monitor activities in Indonesian waters in real-time, detect threats such as enemy submarines or illegal activities, and provide a quick response. A robust IT infrastructure also allows for better coordination between patrol vessels and central command, ensuring that critical information can be relayed and acted upon quickly. Thus, the Indonesian Navy can increase the effectiveness of maritime operations and security in national waters (Franke, 2017).

Air Matra

In the Indonesian Air Force, strengthening the national IT infrastructure allows for more effective integration of AI systems for air surveillance and mission management. Secure local servers ensure that data from radars, drones, and other sensors can be processed quickly and securely, allowing for earlier threat detection and faster response. Reliable IT infrastructure also supports the analysis of flight intelligence data, aiding in mission planning and coordination of air operations. Thus, the Indonesian Air Force can improve preparedness and response capabilities to various air threats (Stone, 2016).

Cyber Matra

Strengthening the national IT infrastructure is crucial for the TNI Matra Cyber, because cyber threats continue to develop and become more sophisticated. The use of robust and secure local servers ensures that sensitive data and cyber defense systems are protected from external cyber attacks. A reliable IT infrastructure enables faster and more effective detection and response to cyberattacks, and supports forensic analysis to identify and address threat sources. By strengthening IT infrastructure, the Cyber Task Force can improve its overall cyber defense capabilities, ensuring that all aspects of military operations are protected from digital threats (Stone, 2016).

Space Matra

For the TNI Matra Antariksa, strengthening the national IT infrastructure allows for more efficient and safe management of satellite data and space operations. AI systems integrated with local servers can be used to monitor and control satellites, ensuring that data collected from space can be processed quickly and securely. A robust IT infrastructure also supports secure communication between satellites and ground stations, as well as allowing for more sophisticated data analysis to detect threats in space, such as space debris

or enemy satellite activity. Thus, the Space Force can increase the effectiveness of space operations and national security (Stone, 2016).

CONCLUSIONS AND RECOMMENDATIONS

Based on the results of the discussion above, the following conclusions were obtained:

The Strength Opportunity (SO) strategy involves the use of artificial intelligence (AI) in improving application security and the integration of AI in defense systems through the Fourth Industrial Revolution (Industry 4.0). This strategy also includes the launch of the Indonesian National Artificial Intelligence Strategy (STRANAS-KA) as the basis for developing experts in the field of AI and collaboration with the private sector to increase defense productivity.

1. First, the use of advanced AI technology in every TNI will improve the overall security of the application. AI technology is able to detect and respond to cyber threats quickly and accurately, strengthening operational capabilities on land, sea, air, cyber, and space.
2. Second, the integration of AI in the defense system through the Fourth Industrial Revolution will increase the efficiency and effectiveness of TNI operations in various dimensions. AI aids in the detection, analysis, and response to threats, strengthens decision-making capabilities in the field, and improves the combat readiness of troops.
3. Third, the launch of STRANAS-KA is the foundation for the development of AI experts in the TNI, improving technical and managerial capabilities in AI to optimize the use of AI technology in defense operations.
4. Finally, collaboration with the private sector enables the development of innovative AI solutions in defense operations, improves operational efficiency, and strengthens national resilience against increasingly complex and sophisticated cyber threats.

ADVANCED RESEARCH

In writing this article the researcher realizes that there are still many shortcomings in terms of language, writing, and form of presentation considering the limited knowledge and abilities of the researchers themselves. Therefore, for the perfection of the article, the researcher expects constructive criticism and suggestions from various parties.

REFERENCES

Allen, G. C., & Chan, T. (2017). "Artificial Intelligence and National Security." Belfer Center for Science and International Affairs.

Bennett, C., & Rajpurkar, P. (2020). An Introduction to Artificial Intelligence in Defense Applications. Defense Innovation Board. Retrieved from Defense Innovation Board

Bijker, W. E., Hughes, T. P., & Pinch, T. (1987). The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology. MIT Press.

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731.

Christensen, C. (2020). "Artificial Intelligence in Military Applications: A Realistic Assessment." Military Review.

Defense Advanced Research Projects Agency (DARPA). (2019). "Artificial Intelligence Exploration (AIE) Program."

Franke, U. E., & Sartre, B. (2017). "Artificial Intelligence in Military Decision-Making." IEEE Intelligent Systems.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

Goodman, M., & Lin, H. (2007). "Toward a Safer and More Secure Cyberspace." National Research Council.

Gollmann, D. (2011). Computer security. John Wiley & Sons.

Huang, P. (2019). "AI in Maritime Defense: Enhancing Situational Awareness." Naval War College Review.

Indonesian Ministry of Research and Technology. (2020). "Indonesian National Strategy for Artificial Intelligence (STRANAS-KA) 2020-2045."

Jurafsky, D., & Martin, J. H. (2008). Speech and Language Processing. Pearson.

Ministry of Defense of the Republic of Indonesia. (2020). "Indonesian National Strategy for Artificial Intelligence (STRANAS-KA) 2020-2045."

Latour, B. (2005). Reassembling the Social: An Introduction to Actor-Network-Theory. Oxford University Press.

Mitchell, T. M. (1997). Machine Learning. McGraw-Hill.

Roff, H. M. (2019). "The Strategic Implications of Military AI." Journal of Strategic Studies.

Russell, S., & Norvig, P. (2016). Artificial Intelligence: A Modern Approach. Pearson.

Smith, M. R., & Marx, L. (1994). Does Technology Drive History? The Dilemma of Technological Determinism. MIT Press.

Stone, P., Brooks, R., Brynjolfsson, E., Calo, R., Etzioni, O., Hager, G., ... & Leyton-Brown, K. (2016). "Artificial Intelligence and Life in 2030." One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel.

Sutton, R. S., & Barto, A. G. (2018). Reinforcement Learning: An Introduction. MIT Press.

Taddeo, M. (2019). "The Limits of AI in Cyber Defense." Journal of Cyber Policy.

Tipton, H. F., & Krause, M. (2012). Information security management handbook. CRC Press.

United Nations Institute for Disarmament Research (UNIDIR). (2022). Artificial Intelligence and International Security. Geneva: UNIDIR Publication.

Weeden, B. (2019). "AI and Space Security: Prospects and Challenges." Astropolitics.

Whitman, M. E., & Mattord, H. J. (2013). Principles of information security. Cengage Learning.