International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.
© 2025 Scholar AI LLC.
https://ijpsat.org/

Vol. 49 No. 1 February 2025, pp. 01-17

SWOT Analysis in Determining Cyber Security Strategy in the Implementation of the Internet of Defense Things (IoDT) 5.0 System in the Defense Industry (PT. Dirgantara Indonesia, PT. Len Industri, and PT. Pindad)

Ra'idah Naufaliana Dewi[1], H.A Danang Rimbawa[2], Bisyron Wahyudi[3]

[1]Cyber Defense Engineering Study Program, Faculty of Defense Science and Technology
The Republic of Indonesia Defense University
Sentul, Bogor
raidah.dewi@tp.idu.ac.id

[2]Cyber Defense Engineering Study Program, Faculty of Defense Science and Technology
The Republic of Indonesia Defense University
Sentul, Bogor
hadr71@idu.ac.id

[3]Cyber Defense Engineering Study Program, Faculty of Defense Science and Technology
The Republic of Indonesia Defense University
Sentul, Bogor
bisyron@gmail.com

Abstract*— This study examines the implementation of the Internet of Defense Things (IoDT) 5.0 within the Indonesian defense industry, focusing on cybersecurity aspects. Through a SWOT analysis, the research identifies internal and external factors influencing the success or challenges of IoDT 5.0 implementation. Data collected via observations and questionnaires at PT. Pindad, PT. Dirgantara Indonesia, and PT. Len Industri in Bandung reveal key insights into the effectiveness of access management processes, incident response in cybersecurity, organizational culture and employee awareness of cybersecurity, the readiness of cybersecurity infrastructure, and the competencies of cybersecurity human resources. The findings highlight the critical need to strengthen access management procedures, enhance employee awareness, improve cybersecurity infrastructure, and develop the skills of cybersecurity professionals to address escalating threats. This research provides valuable insights into the challenges and strategic approaches for advancing IoT 5.0 in Indonesia's defense sector.

***Keywords*—IoDT 5.0, Cyber Security, Defense Industry, SWOT Analysis, Security Infrastructure**

I. INTRODUCTION

The rapid advancements in the digital era have significantly impacted various industrial sectors, introducing the Internet of Things (IoT) as a transformative technology that enables intelligent connectivity between devices and systems. In the defense industry, this evolution has led to the development of the Internet of Defense Things (IoDT), which integrates IoT technology into defense systems to enhance operational effectiveness and efficiency. The latest iteration, IoDT 5.0, represents a major leap forward, incorporating advanced technologies such as artificial intelligence (AI), machine learning (ML), and big data analytics to address increasingly complex operational challenges.

IoDT 5.0 offers immense potential to improve the efficiency and effectiveness of defense operations. However, this heightened connectivity and reliance on advanced technologies also make defense systems more vulnerable to cyber threats. With cyberattacks growing in sophistication and scale, securing IoDT 5.0 systems has become a critical challenge. The defense sector must proactively address these vulnerabilities to safeguard sensitive information and maintain operational integrity in the face of evolving cyber risks.

To effectively implement IoDT 5.0, a comprehensive understanding of its cybersecurity challenges is essential. This research aims to analyze the strengths, weaknesses, opportunities, and threats (SWOT) associated with IoDT 5.0 in the defense industry. By leveraging SWOT analysis, this study seeks to identify the internal and external factors influencing the implementation of IoDT 5.0 and develop strategic recommendations for overcoming cybersecurity challenges while maximizing the benefits of this disruptive technology.

Through a focused evaluation, this research aspires to provide actionable insights that will help organizations in the defense industry adopt IoDT 5.0 securely and effectively, ensuring resilience against potential cyber threats and advancing operational capabilities in a dynamic and challenging environment.

II. Literature review

A. *Theoritical Foundation*

1. Internet of Defense Things (IoDT) 5.0

Not long after the introduction of Industry 4.0, the world is now transitioning towards Industry 5.0, which was first initiated by Japan in 2016 (Nagasato et al., 2018). Industry 5.0 aims to enhance the interaction between humans and technology through the integration of advanced technologies such as Artificial Intelligence (AI), Robotics Process Automation (RPA), Machine Learning, Big Data, and the Internet of Things (IoT), fostering a symbiotic mutualism (Al-Faruqi, 2019). While IoT has already been implemented across various sectors like agriculture, health, defense, transportation, and manufacturing, its transformation into the Industrial Internet of Things (IIoT) in Industry 4.0 has primarily focused on automation in manufacturing. However, Industry 5.0 builds on this foundation by personalizing technology to enhance human capabilities and productivity (Kumar et al., 2022). Within this context, IoT 5.0 represents an evolution of IoT tailored specifically for defense applications, known as the Internet of Defense Things (IoDT). By integrating cutting-edge technologies like AI, machine learning, and big data analytics, IoDT enhances the operational effectiveness of defense systems, enabling faster decision-making, improved efficiency, and automated responses to security threats.

2. Cyber Security

Cybersecurity is the effort to protect digital devices from threats arising from technological advancements and the cyber world, including direct attacks by malicious actors and disruptive software, which can impact productivity, reputation, revenue, and safety (Venkatachary et al., 2018; Daniel et al., 2016). In the context of IoT 5.0, where interconnected defense systems amplify the risks of cyberattacks, cybersecurity becomes crucial to safeguard operations and national security. Effective cybersecurity requires clear policies and regulations as a foundation for governance, guiding organizations in protecting IoT 5.0 systems (Ministry of Defense, 2014). Additionally, the establishment of a dedicated cybersecurity team or Cyber Incident Response Team is essential to address and manage cyber incidents effectively (President of the Republic of Indonesia, 2022). Infrastructure and technology, such as secure networks, encryption, AI, and Big Data analytics, form the backbone of cybersecurity, providing robust protection against threats

(Purbo, 2023). Furthermore, the role of human resources is vital, requiring continuous training and competency development to adapt to the dynamic cyber landscape, alongside fostering a strong cybersecurity culture to enhance individual awareness and organizational resilience in safeguarding information assets (Ministry of Defense, 2014).

3. SWOT Analysis Matrix

SWOT analysis matrix is a strategic planning method used to evaluate the strengths, weaknesses, opportunities, and threats of a project or business, providing a structured framework to assess internal and external factors that influence specific goals (Mariantha, 2018). To understand it more deeply, a SWOT (Strategy Quadrant) analysis diagram is processed as follows so that a precise diagram can be obtained regarding the existing research results, namely what strategies are suggested for the research object as in Figure 1 below:

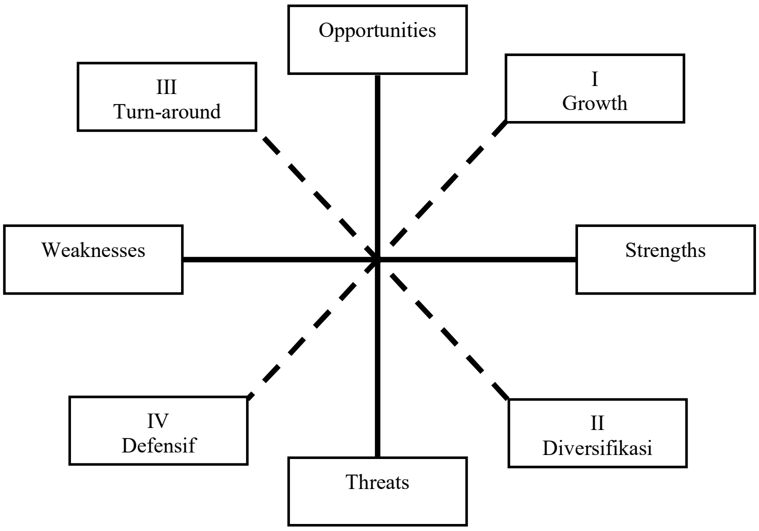

Fig. 1. Diagram (Strategy Quadrant) SWOT Analysis

The description of the SWOT Strategy Quadrant is as follows:

1. QUADRANT 1 : is a very profitable situation. The organization has opportunities and strengths so it can take advantage of existing opportunities. The strategy implemented in this condition is a strategy that supports aggressive growth policies (growth oriented strategy).
2. QUADRANT 2 : despite facing various threats, the organization still has internal strength. The strategy implemented is to use strengths to take advantage of long-term opportunities by means of a diversification strategy (Product/Market).
3. QUADRANT 3 : the organization faces enormous opportunities, but on the other hand faces several internal obstacles/weaknesses. The focus of this organizational strategy is to minimize the company's internal problems so that it can seize better opportunities.
4. QUADRANT 4 : shows a very unfavorable situation, the organization faces various internal threats and weaknesses. Must immediately look for a defensive strategy. (Wiradhana, 2012).

Strengths refer to positive internal attributes that provide a competitive advantage, while weaknesses are internal deficiencies that may hinder success. Opportunities represent external factors that can drive growth or profits, and threats are external challenges that may obstruct progress. By combining internal factors (strengths and weaknesses) with external factors (opportunities and threats) in a SWOT matrix, strategic alternatives such as SO (Strength-Opportunities), ST (Strength-Threats), WO (Weakness-Opportunities), and WT (Weakness-Threats) can be formulated (Rangkuti, 2001). The matrix can produce 4 (four) sets of possible strategic alternatives, as in Table I below:

TABLE I. SWOT MATRIX

EFI / *EFE*	*Strength (S)*	*Weakness (W)*
Opportunity (O)	*Strategy (S+O)* *List strengths to take advantage of existing opportunities*	*Strategy (W+O)* *Register to minimize weaknesses by taking advantage of existing opportunities*
Threat (T)	*Strategy (S+T)* *List of strengths to avoid threats*	*Strategy (W+T)* *Register to minimize weaknesses and avoid threats*

Based on the SWOT Matrix, 4 (four) strategic steps are obtained as follows:

a) SO (Strength-Opportunity) Strategy

1. Leverage advanced cybersecurity technology and infrastructure (S1) to implement clear procedures for managing access and addressing IoT 5.0 system cybersecurity incidents (O1).
2. Utilize a team of competent cybersecurity experts (S2) to enhance employee training and awareness about cybersecurity (O2).

b) ST (Strength-Threat) Strategy

1. Utilize advanced cybersecurity technology and infrastructure (S1) to improve detection, response, and recovery capabilities for IoT 5.0 systems (T2).
2. Rely on a team of competent cybersecurity experts (S2) to develop rapid detection and response strategies for potential cyberattacks (T1).

c) WO (Weakness-Opportunity) Strategy

1. Address weaknesses in cybersecurity policies and unclear procedures (W1, W2) by implementing clear procedures to manage access and handle IoT 5.0 system cybersecurity incidents (O1).
2. Utilize opportunities to improve employee training and education on cybersecurity (O2) to mitigate procedural weaknesses.

d) WT (Weakness-Threat) Strategy

1. Address weaknesses in cybersecurity policies and unclear procedures (W1, W2) to enhance the organization's ability to detect, respond to, and recover from cyberattacks against IoT 5.0 systems (T2).
2. Implement clear procedures to manage access and address IoT 5.0 system cybersecurity incidents (O1) to mitigate procedural vulnerabilities that could be exploited by cyberattacks.

Internal Factor Analysis Summary (IFAS) identifies internal strengths and weaknesses across areas like resources, management, and skills, while External Factor Analysis Summary (EFAS) evaluates external opportunities and threats from macro and micro environments, including regulations, competition, and market trends (David, 2010).

TABLE II. IFAS MATRIX

Internal Strategy Factors	**Questionnaire Data Processing** **(Linkert scale)**	**Weight**	**Ratings**	**Score** **(Weight x Rating)**
Strength (S)	Response (1...n)	Response (1..n)/(X1+X2)	1..5	Weight x Rating (1...Zn)
Amount	**X1**	**Y1**		**Z1**
Weakness (W)	Response (1...n)	Response (1..n)/(X1+X2)	1...5	Weight x Rating (1...Zn)
Amount	**X2**	**Y2**		**Z2**
Total	**X1+X2**	**Y1+Y2 = 1**		**Z1+Z2**

TABLE III. EFAS MATRIX

External Strategy Factors	**Questionnaire Data Processing (Linkert scale)**	**Weight**	**Ratings**	**Score** **(Weight x Rating)**
Chance (O)	Response (1...n)	Response (1..n)/(A1+A2)	1..5	Weight x Rating (1...Cn)
Amount	**A1**	**B1**		**C1**
Threat (T)	Response (1...n)	Response (1..n)/(A1+A2)	1...5	Weight x Rating (1...Cn)
Amount	**A2**	**B2**		**C2**
Total	**A1+A2**	**B1+B2 = 1**		**C1+C2**

This research applies SWOT analysis to assess the factors influencing cybersecurity in the implementation of IoT 5.0, offering valuable insights for strategic planning and decision-making.

B. Previoud Research Results

No.	Researcher, Year, Tittle	Research Purposes	Research Summary	Research Summary	
				Equality	Difference
1	Agus Kurniati, S.ST, MM (2019). SWOT Analysis in Determining Cyber and Password Security Training Strategies.	Identify strengths and weaknesses (internal environment), opportunities and threats (external environment) in organizing training.	Uses SWOT analysis to formulate strategies for cyber security training.	Research methods and SWOT analysis.	Research objectives and locus.
2	Eko Budi, Dwi Wira, Ardian Infantono (2021). Strategy for Strengthening Cyber Security to Realize National Security in the Era of Society 5.0.	Get an overview of cybercrime, its future challenges, and strategies for strengthening cyber security in Indonesia.	Explores cyber security to realize national security in Society 5.0.	The same Society 5.0 concept as IoDT 5.0.	Analysis method.
3	Muhammad Haikal Kautsar, et al. (2019). SWOT Analysis of PT. Business Line Innovation. Pindad (Persero): Cyber Security Services.	Conduct a strategy analysis of PT. PINDAD (Persero) in developing its new products.	Uses SWOT and QSPM approaches to analyze strategies for innovation.	SWOT analysis.	Research objectives and locus.
4	Janiah, S. (2019). Strategic Management EFE-IFE Matrix, SWOT Analysis, Competitive Profile Matrix (CPM) and BCG Matrix at Pt Yamaha.	Analyze strategic management carried out at PT YAMAHA.	Explores various strategic management tools, including SWOT analysis.	SWOT analysis method.	Research objectives and locus.
5	Mahira, DF, et al. (2020). Strengthening Multistakeholder Integrated through Shared Responsibility in the Face of Cyber Attacks Threat.	Focus on realizing a cyber resilience system through integrated multi-party strengthening with shared responsibility.	Explains how shared responsibility strengthens cyber resilience.	Realizing cyber security.	The analysis method used.
6	Mashuri, M., & Nurjannah, D. (2020). SWOT Analysis as a Strategy to Increase Competitiveness.	Determine how SWOT analysis increases competitiveness and identifies obstacles.	Examines SWOT analysis in the context of competitiveness in banking.	Research methods and SWOT analysis.	Research objectives and locus.

7	Arfianti (2017). SWOT Analysis in Increasing Competitiveness at PT Trimega Syariah Makassar Branch Office.	Identify the role of SWOT analysis in increasing competitiveness.	Focuses on SWOT analysis for competitive advantage in the banking sector.	SWOT analysis.	Research objectives and locus.

C. Framework of Thought

The framework for this research is developed based on the problem's background, supported by theoretical foundations and previous studies, serving as a guide to systematically structure the research methods. It acts as a conceptual model linking theories to key factors related to IoT 5.0. The company is encouraged to implement a SWOT analysis (strengths, weaknesses, opportunities, and threats) to evaluate internal and external conditions. This includes identifying product strengths and weaknesses, addressing competition threats, and leveraging opportunities to enhance market share. This conceptual framework provides a structured approach to addressing critical issues in the study.

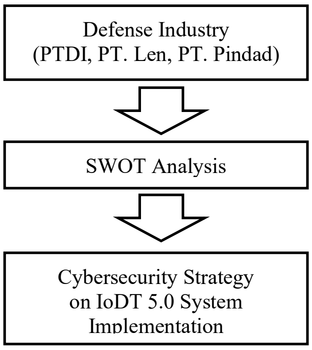

Fig. 2. Framework of Thought

III. RESEARCH METHODOLOGY

A. Research Methods and Design

1. Research Methods

The quantitative descriptive research method is designed to objectively illustrate or describe a situation through numerical data. This process involves data collection, interpretation, and presentation of results (Arikunto, 2006). In this study, the approach is quantitative descriptive, meaning the data gathered is numerical, processed, and presented to accurately depict the observed object.

2. Research Design

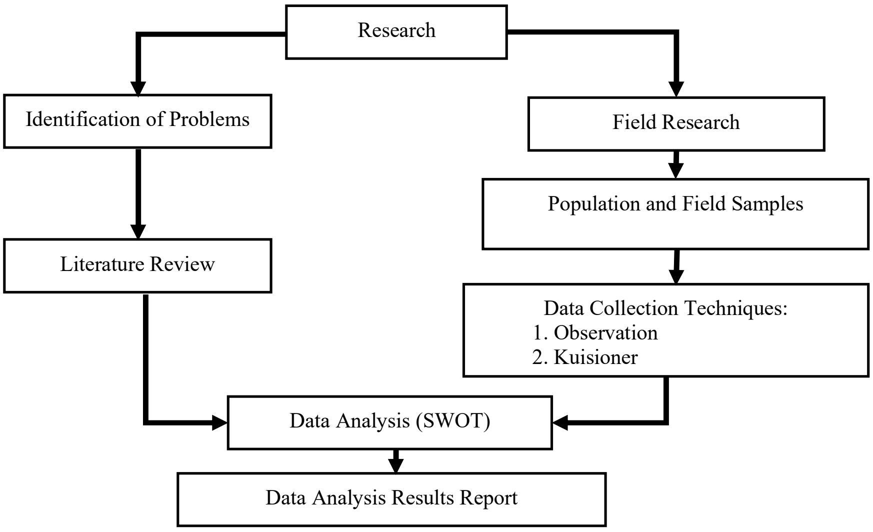
Research
Identification of Problems
Field Research
Population and Field Samples
Literature Review
Data Collection Techniques:
1. Observation
2. Kuisioner
Data Analysis (SWOT)
Data Analysis Results Report

Fig. 3. Research Design

B. Place and Time of Research

The research was conducted within the defense industry, specifically at PT. Pindad, PT. Dirgantara Indonesia, and PT. Len Industri, located in Bandung. This study took place over a short period, from March 6 to 7, 2024, as part of the Domestic Work Lecture (KKDN) activities.

C. Population and Research Sample

This research utilized data from internal company sources, including management and staff from the Systems Engineer and Information Technology units of PT. Pindad, PT. Dirgantara Indonesia, and PT. Len Industri, to explore cyber security strategies in IoT system implementation within the defense industry. Data was collected through primary sources, including questionnaires distributed to respondents, and secondary sources, such as company websites.

D. Data Collection Techniques

Data collection is a crucial step in research, as its primary purpose is to obtain reliable data (Sugiyono, 2003). In this study, three techniques were utilized to gather data. First, a literature review was conducted by sourcing information from books, journals, the internet, and other references relevant to the research topic. This approach provided foundational knowledge and context for the study.

Second, direct observation was employed to collect data by observing physical symptoms and processes at the research site. Lastly, questionnaires were distributed to eight respondents from defense industry companies. These questionnaires served as an initial step in analyzing the situation and making informed decisions regarding cyber security strategies.

E. Research Instrument

The indicators provided to respondents in this research represent the variables of the SWOT method, divided into internal and external factors. Internal factors include strengths (S) and weaknesses (W). Strengths encompass aspects such as the availability of advanced cybersecurity technology and infrastructure for IoT 5.0 systems (S1), a team of experienced cybersecurity experts (S2), and clear procedures for managing system access (S3) and handling cybersecurity incidents (S4). Additionally, employee training on cybersecurity for IoT 5.0 systems is highlighted as a significant strength (S5). On the other hand, weaknesses include the lack of a strong cybersecurity culture among employees (W1), infrequent penetration testing and audits to address system vulnerabilities (W2), the absence of comprehensive cybersecurity policies (W3), unclear access management procedures (W4), and the lack of mandatory regular cybersecurity training for employees (W5). The research instrument of Internal Factor can be shown in Table IV below:

TABLE IV. INTERNAL FACTORS TABLE

No	Strength
S1	Has the latest cybersecurity technology and infrastructure to protect the IoT 5.0 system
S2	Has a team of competent and experienced cybersecurity experts in securing the IoT 5.0 system
S3	Have clear procedures for managing access to the IoT 5.0 system
S4	Have clear procedures for handling cybersecurity incidents involving IoT 5.0 systems
S5	Employees who have access to the IoDT 5.0 system have received adequate training on cybersecurity
No	**Weakness**
W1	The cyber security culture is still not strong and some employees do not fully understand the importance of cyber security
W2	It is rare to conduct penetration tests and cybersecurity audits to identify and address vulnerabilities in IoT 5.0 systems
W3	The IoT 5.0 system cybersecurity policy is not yet comprehensive and clear
W4	Lacks clear procedures for managing access to the IoT 5.0 system
W5	Employees are not required to take regular cyber security training

External factors are categorized into opportunities (O) and threats (T). Opportunities focus on enhancing security through advanced cybersecurity technologies (O1), investments in technology and training (O2), and implementing clear procedures for access management (O3) and incident handling (O4). Moreover, improving cybersecurity education and training programs (O5) and ensuring continuous updates to employee knowledge through ongoing training (O6) are seen as valuable opportunities. Conversely, threats include the ever-present risk of cyberattacks targeting IoT 5.0 systems (T1), the potential involvement of various threat actors such as hackers, criminal groups, or other nations (T2), and the risks these attacks pose to national security (T3). Additionally, organizations' current unpreparedness to handle cyberattacks (T4) and the need to improve their detection, response, and recovery capabilities (T5) are identified as significant external challenges. The research instrument of External Factors can be shown in Table V below:

TABLE V. EXTERNAL FACTORS TABLE

No	Opportunity
O1	Implementing the latest cybersecurity technologies and practices can significantly improve the security of IoT 5.0 systems in Organizations
O2	Organizations can improve their ability to secure IoT 5.0 systems by investing in cybersecurity technology and training
O3	Implementing clear procedures to manage access to IoT 5.0 systems can help Organizations limit access and prevent security breaches
O4	Developing clear procedures for handling cybersecurity incidents involving IoT 5.0 systems can help Organizations respond to incidents more quickly and effectively
O5	Improving training and education about cyber security for my Organization's employees can increase their awareness and understanding of the importance of cyber security

O6	Implementing an ongoing cybersecurity training program can help my Organization ensure that its employees are always up-to-date with the latest cybersecurity practices
No	**Threat**
T1	Cyberattacks against IoT 5.0 systems in Organizations can occur at any time
T2	Cyber attacks against IoT 5.0 systems in organizations can be carried out by various parties, such as hackers, criminal groups, or other countries
T3	A successful cyberattack against an Organization's IoT 5.0 system could endanger national security
T4	Organizations are not yet fully prepared to deal with cyberattacks against IoT 5.0 systems
T5	Organizations need to improve their ability to detect, respond, and recover from cyberattacks against IoT 5.0 systems

IV. Research Results and Discussion

A. General Description of Research Objects

State-Owned Enterprises (BUMN) in Indonesia have a vision of becoming key drivers of the national economy. This vision was materialized with the establishment of the Defense Industry BUMN Holding, known as Defense Industry Indonesia (DEFEND ID). Officially inaugurated on April 20, 2022, by President Joko Widodo at the PT. PAL Indonesia Submarine Hangar in Surabaya, DEFEND ID is a collaboration of five state-owned companies in the defense sector. These companies include PT. Len Industri Industri (Persero), serving as the parent company, along with PT. Pindad, PT. Dirgantara Indonesia (PTDI), PT. PAL Indonesia, and PT Dahana. DEFEND ID aims to create a competitive and independent Indonesian defense industry capable of competing in the global market, targeting inclusion in the Top 50 Defense Global Companies by 2024.

PT. Len Industri (Persero), established in 1965 as the National Electrotechnical Institute (LEN), transitioned into a state-owned enterprise in 1991. Operating under the Ministry of State-Owned Enterprises, PT. Len Industri focuses on electronics for industry and infrastructure, excelling in various fields. These include railway signaling systems, urban transportation projects like LRT systems, telecommunications infrastructure, defense electronics (radar, tactical radios, and Combat Management Systems), solar power plants, and weather and earthquake monitoring systems. As part of the Manufacturing Industry Cluster in the defense sub-sector, PT. Len Industri leads efforts to accelerate the integration of defense industry BUMNs under DEFEND ID. PT. Len Industri’s vision is to become a trusted world-class technology company, supported by innovative solutions and a commitment to enhancing national sovereignty and quality of life.

PT. Dirgantara Indonesia (PTDI), founded in 1976, is one of Asia's leading aerospace companies. Based in Bandung, PTDI specializes in designing, manufacturing, and servicing aircraft for both civilian and military purposes. It has delivered nearly 400 aircraft to 50 operators worldwide, including models like the CN235 for transportation and maritime surveillance. PTDI's vision is to become the market leader in middle and light-class turboprop aircraft in the Asia Pacific region, with a mission to provide high-quality, cost-competitive products and services while maintaining strategic alliances with global aerospace leaders.

PT. Pindad (Persero) is another significant player in the defense industry, focusing on manufacturing and developing military equipment (Alutsista) and commercial products. The company produces a wide range of defense and non-defense equipment, offers services in industries such as mining and construction, and engages in trading activities. PT. Pindad envisions becoming a Top 100 global defense company by 2024 by offering innovative, high-quality product solutions through strategic partnerships. Its mission is to integrate efforts in defense and industrial equipment to support national development and bolster national security.

B. Research Results

Based on data analysis using the Internal Factor Analysis Strategy (IFAS) and External Factor Analysis Strategy (EFAS) matrices, the study identified the weight values and scores for strengths, weaknesses, opportunities, and threats associated with cybersecurity strategies in the implementation of IoDT 5.0. The results of the IFAS analysis show in Table III, provide insights into the internal factors. For strengths, the total weight value was calculated at 0.42, with a total score of 1.58, while for weaknesses, the total weight value reached 0.58, with a total score of 1.99. These results highlight the relative prominence of weaknesses compared to strengths within the internal factors of the cybersecurity strategy.

TABLE VI. IFAS MATRIX RESULTS

No	Internal factors	Questionnaire Data Processing	Ratings	Weight (%)	Score (B x R)
S1	My organization has state-of-the-art cybersecurity technology and infrastructure to protect IoT 5.0 systems	26	4	0.09	0.35
S2	My organization has a team of cybersecurity experts who are competent and experienced in securing IoT 5.0 systems	29	4	0.10	0.39
S3	My organization has clear procedures for managing access to the IoT 5.0 system	20	4	0.07	0.27
S4	My organization has clear procedures for handling cybersecurity incidents involving IoT 5.0 systems	25	4	0.08	0.34
S5	My Organization's employees who have access to the IoT 5.0 system have received adequate training on cybersecurity	24	3	0.08	0.24
	Total Strengths	**124**	**19**	**0.42**	**1.58**
W1	**The cyber security culture in my organization is still not strong and some employees do not fully understand the importance of cyber security**	38	3	0.13	0.38
W2	My organization rarely performs penetration tests and cybersecurity audits to identify and address vulnerabilities in IoT 5.0 systems	33	3	0.11	0.33
W3	My organization's cybersecurity policy for the IoT 5.0 system is not yet comprehensive and clear	34	4	0.11	0.46
W4	My organization does not have clear procedures for managing access to the IoT 5.0 system	38	4	0.13	0.51
W5	My Organization's employees are not required to undergo regular cybersecurity training	31	3	0.10	0.31
	Total Weaknesses	**174**	**17**	**0.58**	**1.99**
	Total SW	**298**	**36**	**1.00**	**3.58**
	SW Difference				**-0.41**

The EFAS analysis, evaluates the external factors of opportunities and threats. In Table IV, the analysis revealed a total weight value of 0.58 and a total score of 2.12, indicating significant potential for leveraging external opportunities in strengthening cybersecurity strategies for IoDT 5.0 implementation. On the other hand, the threats carried a total weight value of 0.42, with a corresponding score of 1.45, illustrating the challenges that must be mitigated to ensure robust cybersecurity.

TABLE VII. EFAS MATRIX RESULTS

No	External Factors	Questionnaire Data Processing	Ratings	Weight (%)	Score
O1	Implementing the latest cybersecurity technologies and practices can significantly improve the security of IoT 5.0 systems in my Organization	38	3	0.09	0.28
O2	My organization can improve its ability to secure IoT 5.0 systems by investing in cybersecurity technology and training	38	3	0.09	0.28
O3	Implementing clear procedures for managing access to IoT 5.0 systems can help my Organization limit access and prevent security breaches	40	4	0.10	0.39
O4	Developing clear procedures for handling cybersecurity incidents involving IoT 5.0 systems can help my Organization respond to incidents more quickly and effectively	40	4	0.10	0.39
O5	Improving training and education about cyber security for my Organization's employees can increase their awareness and understanding of the importance of cyber security	40	4	0.10	0.39
O6	Implementing an ongoing cybersecurity training program can help my Organization ensure that its employees are always up-to-date with the latest cybersecurity practices	40	4	0.10	0.39
	Total Opportunities	236	22	0.58	2.12
T1	A cyberattack against the IoT 5.0 system in my Organization could occur at any time	36	4	0.09	0.35
T2	Cyberattacks against the IoT 5.0 system in my Organization can be carried out by various parties, such as hackers, criminal groups, or other countries	36	3	0.09	0.26
T3	A successful cyberattack against an IoT 5.0 system at my Organization could compromise national security	34	3	0.08	0.25
T4	My organization is not fully prepared to deal with cyberattacks against IoT 5.0 systems	30	3	0.07	0.22
T5	My organization needs to improve its ability to detect, respond, and recover from cyberattacks against IoT 5.0 systems	38	4	0.09	0.37
	Total Threats	174	17	0.42	1.45
	Total SW	410	39	1.00	3.57
	OT Difference				-1.45

These findings underline the importance of strategically addressing internal weaknesses and external threats while capitalizing on strengths and opportunities. By carefully analyzing these factors, organizations can develop more effective and sustainable cybersecurity strategies for the IoDT 5.0 system.

C. Discussion

1) SWOT Quadrant Diagram Analysis

Based on the data processing results using the IFAS and EFAS Matrices, the current state of the cybersecurity strategy for IoDT 5.0 implementation is positioned at the coordinates **(x, y) = (-0.41, -1.45)**. This position falls into **Quadrant 4** of the SWOT Analysis Diagram. Quadrant 4 signifies the need for a **Defensive Strategy**, indicating that the organization is facing significant challenges in its cybersecurity approach. Internal weaknesses must be addressed while simultaneously managing substantial external threats, making this quadrant particularly challenging to navigate.

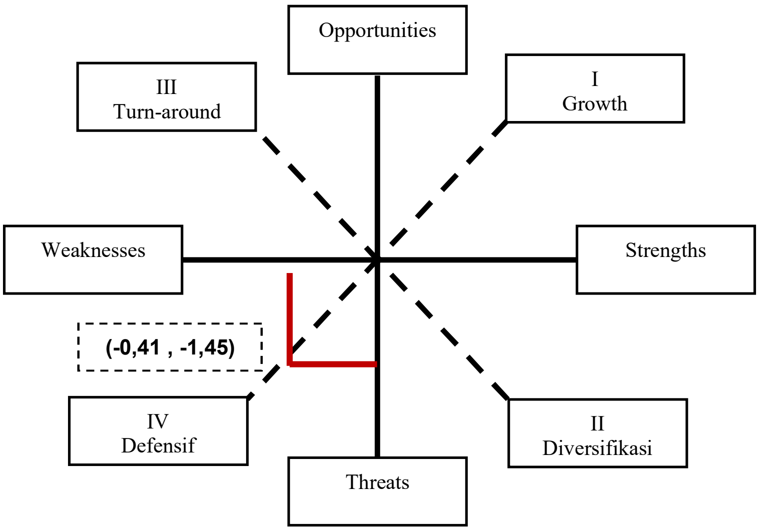

Fig. 4. SWOT Analysis Quadrant Diagram

2) SWOT Matrix Analysis

The IFAS and EFAS values have been combined into a SWOT analysis matrix, creating strategy alternatives based on internal and external factors. The formulated strategies fall into four categories: SO (Strength-Opportunity), ST (Strength-Threat), WO (Weakness-Opportunity), and WT (Weakness-Threat). The following are the proposed strategy combinations derived:

TABLE VIII. SWOT MATRIX

EFI *EFE*	*Strength (S)* 1. ***Has the latest cybersecurity technology and infrastructure*** 2. ***Has a team of competent and experienced cyber security experts***	*Weakness (W)* 1. ***The IoT 5.0 system cybersecurity policy is not yet comprehensive and clear*** 2. ***Lacks clear procedures for managing access to the IoT 5.0 system***
Chance (O) 1. ***Implement clear procedures to manage access and handle IoT 5.0 system cybersecurity incidents*** 2. ***Implementation and improvement of training and education on cyber security for Organization employees***	*Strategy (S+O) = 3.70* 1. ***Leverage strengths in state-of-the-art cybersecurity technology and infrastructure (S1) to implement clear procedures for managing access and handling IoT 5.0 (O1) system cybersecurity incidents.*** 2. ***Using a team of competent cyber security experts (S2) to improve training and education about cyber security for employees (O2).***	*Strategy (W+O) = 4.11* 1. ***Address weaknesses in cybersecurity policies and unclear procedures (W1, W2) by implementing clear procedures to manage access and handle IoT 5.0 system cybersecurity incidents (O1).*** 2. ***Taking advantage of opportunities to improve training and education on cyber security for employees (O2) to address weaknesses in procedures.***
Threat (T) 1. ***Cyberattacks against IoT 5.0 systems in Organizations can occur at any time*** 2. ***Organizations need to improve their ability to detect, respond, and recover from cyberattacks against IoT 5.0 systems***	*Strategy (S+T) = 3.04* 1. ***Leverage strengths in advanced cybersecurity technology and infrastructure (S1) to enhance detection, response, and recovery capabilities from cyberattacks against IoT 5.0 (T2) systems.*** 2. ***Using a team of competent cybersecurity experts (S2) to develop rapid detection and response strategies for cyber attacks that can occur at any time (T1).***	*Strategy (W+T) = 3.45* 1. ***Address weaknesses in cybersecurity policies and unclear procedures (W1, W2) to improve detection, response, and recovery capabilities from cyberattacks against IoT 5.0 systems (T2).*** 2. ***Implement clear procedures to manage access and handle IoT 5.0 (O1) system cybersecurity incidents to address weaknesses in procedures that could be exploited by cyber attacks.***

Based on the SWOT Matrix (Table VIII), the proposed sequence of alternative strategies that can be used for cyber security in the implementation of IoDT 5.0 is as follows:

a. W+O Strategy

1. Address weaknesses in cybersecurity policies and unclear procedures (W1, W2) by implementing clear procedures to manage access and handle IoT 5.0 system cybersecurity incidents (O1).
2. Taking advantage of opportunities to improve training and education on cyber security for employees (O2) to address weaknesses in procedures.

b. S+O Strategy

1. Leverage strengths in state-of-the-art cybersecurity technology and infrastructure (S1) to implement clear procedures for managing access and handling IoT 5.0 (O1) system cybersecurity incidents.
2. Using a team of competent cyber security experts (S2) to improve training and education about cyber security for employees (O2).

c. W+T Strategy

1. Address weaknesses in cybersecurity policies and unclear procedures (W1, W2) to improve detection, response, and recovery capabilities from cyberattacks against IoT 5.0 systems (T2).
2. Implement clear procedures to manage access and handle IoT 5.0 (O1) system cybersecurity incidents to address weaknesses in procedures that could be exploited by cyber attacks.

d. S+T Strategy

1. Leverage strengths in advanced cybersecurity technology and infrastructure (S1) to enhance the detection, response, and recovery capabilities of IoT 5.0 (T2) systems.
2. Using a team of competent cybersecurity experts (S2) to develop rapid detection and response strategies for cyber attacks that can occur at any time (T1).

3) Proposed Strategic Prioritization

The recommended prioritization of strategies begins with the WO Strategy, as it focuses on addressing internal weaknesses while leveraging external opportunities to improve overall cybersecurity readiness. This is followed by the SO Strategy, which emphasizes maximizing organizational strengths to capitalize on opportunities. Finally, the WT and ST strategies are implemented to ensure that internal vulnerabilities and external threats are comprehensively managed.

V. CONCLUSIONS AND RECOMMENDATIONS

A. Conclusion

The research on cybersecurity in the implementation of Internet of Defense Things (IoDT) 5.0 within the Indonesian defense industry (PT. Len Industri, PT. Dirgantara Indonesia, and PT. Pindad) highlights several key findings. The effectiveness of access management and incident response processes plays a vital role in minimizing risks, necessitating clear and efficient procedures. Organizations must also foster a strong cybersecurity culture and enhance employee awareness through continuous training and education. The current state of the cybersecurity strategy, positioned at coordinates (-0.41, -1.45), underscores the need for concrete actions to address vulnerabilities and strengthen infrastructure. Additionally, the competency of cybersecurity professionals is critical, requiring enhanced skills and strategies for rapid detection and response to evolving threats.

B. Recomendation

Based on the research findings, theoretical and implementation recommendations are proposed to enhance cybersecurity in the Indonesian defense industry. Theoretically, future research should focus on developing specific detection and response methods for cyberattacks on IoT 5.0 systems, studying psychological factors influencing employee cybersecurity awareness, and evaluating the effectiveness of existing cybersecurity policies in defense organizations. For practical implementation, it is recommended to establish stricter cybersecurity policies, conduct regular employee training on cybersecurity best practices, and collaborate with research institutions and industry to develop advanced, adaptive cybersecurity technologies. This study, conducted as part of the Domestic Work Lecture (KKDN), aims to contribute positively to strengthening cybersecurity in the Indonesian defense industry and society.

REFERENCES

[1] President of the Republic of Indonesia, "Presidential Regulation of the Republic of Indonesia Number 82 of 2022 concerning Protection of Vital Information Infrastructure," 2022.

[2] Ministry of Defense, "Regulation of the Minister of Defense of the Republic of Indonesia Number 82 of 2014 concerning Cyber Defense Guidelines," Ministry of Defense of the Republic of Indonesia, 2014.

[3] Kurniati, "SWOT Analysis in Determining Cyber and Password Security Training Strategies," *Journal of Commerce Scholars*, vol. 3, no. 2, pp. 73–86, Nov. 2019.

[4] E. Budi, D. Wira, and A. Infantono, "Strategy for Strengthening Cyber Security to Realize National Security in the Era of Society 5.0," *Proceedings of the Indonesian National Science Technology and Innovation Seminar (SENASTINDO)*, vol. 3, pp. 223–234, Dec. 21, 2021. [Online]. Available: https://doi.org/10.54706/senastindo.v3.2021.141

[5] N. Munasyaroh, M.H. Kautsar, P.A. Fadhilah, I.Y. Utama, and S. Supandi, "SWOT Analysis of PT. Pindad (Persero) Business Line Innovation: Cyber Security Services," *Defendonesia*, vol. 4, no. 1, pp. 1–10, Sep. 19, 2019. [Online]. Available: https://doi.org/10.54755/defendonesia.v4i1.76

[6] S. Janiah, "Strategic Management Effect-Ife Matrix, SWOT Analysis, Competitive Profile Matrix (CPM) and BCG Matrix at Pt Yamaha," *Journal of Information Systems Management Economics*, vol. 1, no. 2, pp. 188–196, Dec. 31, 2019. [Online]. Available: https://doi.org/10.31933/jemsi.v1i2.69

[7] D.F. Mahira, D.S. Rohmahwatin, and N.D. Suciningtyas, "Strengthening Multistakeholder Integrated through Shared Responsibility in the Face of Cyber Attacks Threat," *Lex Scientia Law Review*, vol. 4, no. 1, pp. 63–74, May 8, 2020. [Online]. Available: https://doi.org/10.15294/lesrev.v4i1.38191

[8] M. Mashuri and D. Nurjannah, "SWOT Analysis as a Strategy to Increase Competitiveness," *JPS (Journal of Islamic Banking)*, vol. 1, no. 1, pp. 97–112, Apr. 13, 2020. [Online]. Available: https://doi.org/10.46367/jps.v1i1.205

[9] ARFIANTI, "SWOT Analysis in Increasing Competitiveness at Pt. Trimega Syariah Makassar Branch Office," 2017.

[10] Sugiyono, *Qualitative, Quantitative, R&D Research Methods*, 1st ed., Jakarta: Alphabeta, 2003.

[11] Sugiyono, *Business Research Methods (Quantitative, Qualitative, R&D Approaches)*, Bandung: Alpha Beta, 2013.

[12] L. Sutandar, "Strategic Management Analysis at PT. Semeru Teknik in Surabaya," *AGORA*, 2017.

[13] S. Arikunto, *Research Procedures: A Practical Approach*, 6th ed., rev. 13. Rineka Cipta, 2006.

[14] S.K. Venkatachary, J. Prasad, and R. Samikannu, "Cybersecurity and Cyber Terrorism - in Energy Sector: A Review," *Journal of Cyber Security Technology*, 2018.

[15] D. Ani, U.P. He, H.M. & Tiwari, A., "Review of Cybersecurity Issues in Industrial Critical Manufacturing: Manufacturing in Perspective," *Journal of Cyber Security Technology*, 2017.

[16] C. Rahmawati, "Indonesian Cyber Security Challenges and Threats in the Era of Industrial Revolution 4.0," Nov. 17, 2020. [Online]. Available: https://aau.e-journal.id/senastindo/article/view/116

[17] I.A. Fauzan, "Cyber Security in Indonesia: Building Digital Defense in the Era of Society 5.0," *Kompasiana*, Dec. 18, 2023. [Online]. Available: https://www.kompasiana.com/ibnu1030/658060c312d50f6ea21f9d22/keamanan-cyber-di-indonesia-membangun-perlahan-digital-diera-community-5-0

[18] H. Dwipratama, "The Potential of Dual-Use Technological Disruption in Creating an Advanced, Strong, Independent and Competitive Defense Industry," *Kemhan.go.id*, Sep. 8, 2023. [Online]. Available: https://www.kemhan.go.id/pothan/2023/09/08/potensi-dual-usedisrup-technology-dalam-mewujudkan-industri-perlahan-yang-majukuat-independent-and-powerful-competitive.html

[19] O. Purbo, “Cyber Security: Infrastructure and Technology,” *LinkedIn*, May 30, 2023. [Online]. Available: https://id.linkedin.com/pulse/cyber-security-infrastructure-dantechnology-onno-purbo

[20] DEFEND ID, “DEFEND ID: Transformation Increases Defense Industry Contribution to the Nation,” *Holding of Defense ID*, 2022. [Online]. Available: https://www.len.co.id/defend-id-transformation-angkatkan-kontributindustri-perlahan-kepada-negara/

[21] PT. Len Industri, “PT. Len Industri,” 2024. [Online]. Available: https://www.len.co.id/

[22] PTDI, “PT. Indonesian Aerospace (PTDI),” 2024. [Online]. Available: https://www.indonesian-aerospace.com/id

[23] PT. Pindad, “PT Profile,” *Pindad*, 2024. [Online]. Available: https://pindad.com

[24] I. Kurniawan, “IFAS-EFAS for Strategy Planning,” *School of Information Systems*, Feb. 5, 2021. [Online]. Available: https://sis.binus.ac.id/2021/02/05/ifas-efasuntuk-strategy-planning/