CYBER WARFARE THREATS AND ANALYZING READINESS OF THE INDONESIAN NAVY IN PRIORITIZING VARIABLES

Rakam[1], Choirul Imron[2], Joko Purnomo[3], Priyadi Hartoko[4]

[1]Analysis Systems and Research of OperationsIndonesian Naval Technology College,
Bumimoro-Morokrembangan, Surabaya 60187, Indonesia
Rakam54@gmail.com

ABSTRACT

The advancement of information technology has greatly impacted various aspects of human life, including the Indonesian Navy. This progress has given rise to the concept of Cyber Warfare, which involves conducting warfare through information technology. Cyber warfare refers to actions taken by a country or international organization to attack and undermine another country's computer or information networks, typically through means like viruses or denial of service attacks.In light of these circumstances and challenges, the authors undertook an analysis to assess the readiness of the Indonesian Navy in dealing with the threat of cyber attacks, both domestically and internationally. This research employed cyber warfare threat modelling, which involved weighing and prioritizing key variables such as offensive cyber operations, cyber espionage operations, and cyber support. The objective of this study was to develop a Cyber Warfare threat model to support the responsibilities of the Indonesian Navy. Data processing for this research involved collecting relevant data from activities conducted at Satsiberal Headquarters, which was then analyzed using Fuzzy weighting. Additionally, the Dynamic System modelling method was employed to ascertain the interrelationships between variables and simulate the best alternative scenario. The results of the modellingg and simulation provided valuable insights for addressing the cyber warfare threat effectively

Keywords**:** *Cyber Warfare Threats, Indonesian Navy, Dynamic System*.

1. INTRODUCTION.

Based on Law Number 34 of 2004 concerning the TNI (Indonesian National Army) Article 7 discusses the main tasks of the TNI, namely upholding state sovereignty, maintaining the territorial integrity of the Unitary State of the Republic of Indonesia based on Pancasila and the 1945 Constitution of the Republic of Indonesia, and protecting the entire nation of Indonesia and all of Indonesia's bloodshed from threats and disturbances to the integrity of the nation and state. The main tasks referred to in paragraph (1) are carried out through military operations for war and military operations other than war, namely to overcome armed separatist movements, overcome armed rebellions, and overcome acts of terrorism. The Navy as an integral part of the TNI, carries out the duties of the TNI in the field of defense, including uphold the law and maintaining security in the sea area of national jurisdiction in accordance with ratified national and international legal provisions, carrying out naval diplomacy tasks in order to support foreign policy policies set by the government, carry out TNI duties in building and developing maritime dimension forces, and carry out the defense of maritime defense areas. The Indonesian Navy is always required to be able to adapt to changes in the environment that occur, especially in facing increasingly severe threats, disturbances, challenges and obstacles in the future. carry out the diplomatic duties of the Navy in order to support the foreign policy policies set by the government, carry out the duties of the TNI in the development and development of maritime dimension forces, and carry out the empowerment of the maritime defense area. The Indonesian Navy is always required to be able to adapt to changes in the environment that occur, especially in facing

increasingly severe threats, disturbances, challenges and obstacles in the future. carry out the diplomatic duties of the Navy in order to support the foreign policy policies set by the government, carry out the duties of the TNI in the development and development of maritime dimension forces, and carry out the empowerment of the maritime defense area. The Indonesian Navy is always required to be able to adapt to changes in the environment that occur, especially in facing increasingly severe threats, disturbances, challenges and obstacles in the future.

Based on the situation and problems above, the authors conducted an analysis regarding the readiness of the Indonesian Navy in facing the threat of cyber attacks, both from within the country and from abroad. Where in this research carried out using cyber warfare threat modeling by carrying out weighting and prioritization on the variables of offensive cyber operation (aspects of enforcement), offensive cyber operations (aspects of defense), espionage cyber operations (aspects of intelligence), cyber support using a system approach and modeling dynamic. The advantage of using the system dynamic approach is that the dynamic system has a very good ability to explain the behavior and characteristics of the system being observed and can explain the causal relationship and consequences of changing the state of each variable properly and with the simulation concept it has. Modeling using a dynamic system also has flexibility in its application and also does not interfere with the real system being observed.

2. MATERIALS/METHODS

2.1 Cyber Theory.

The government needs to cooperate with other countries to build global security. One country may not be able to protect itself in dealing with this global threat. Cooperation between countries is also expected to be able to trigger a regulation in the field of cyber or cyber law that is stronger and has a global effect. With the existence of strict cyber laws in the international world, it would be possible to reduce the rampant crime in the cyber world. Before this is implemented, it would be wiser for Indonesia to reorganize its mastery of technology and make specific laws regarding cyber threats. Several countries already have special units of cyber troops in the defense and security of a country. The agency or organization is tasked with compiling all defense efforts and counterattacks against security in the cyber world and its network systems. Seeing the strengths and threats that can occur due to advances in information technology, many countries have begun to build cyber warfare naval forces.

2.2 Cyber Warfare.

Cyber warfare is hacking or data theft through internet/computer/cyber networks based on political motivation with the aim of sabotage or espionage against certain interests. Meanwhile, according to Richard A. Clarke in May 2010 in his book Cyber Warfare is an action by a state/nation to penetrate another nation's computer or network with the aim of causing damage or disruption. While cyber warfare in the global political sphere can be understood as a political action that involves the ability of computer hacking to achieve the goals of the owner of the interest, which among other things can be done through activities such as sabotage and espionage.

Cyber warfare is the latest form of war that uses computer networks and the internet or cyberspace in a strategy of defense or attack on the opponent's information system. Cyber warfare is also known as war which refers to the use of www (world wide web) facilities and computer networks to wage war in cyberspace. Today's cyber warfare activities can be included in the category of low-level information warfare, which in the next few years may be considered as true information warfare. As a form

of information warfare and cyber warfare activities is the use of information technology, communications and the internet to wage war in cyberspace. The internet system is strategically very vulnerable to disruption or attack, and it is very difficult to defend against attacks and distractions, so preparation, vigilance and layered defense are needed. The tactics and strategies used can be in the form of espionage, propaganda, stopping internet operations, modifying data and manipulating infrastructure, and will continue to grow, all of this will be very detrimental and weaken a country.

2.3 Cyber Warfare Threats

Until now cyber security experts in various parts of the world continue to try to defend computer systems from online crime. Cyber attacks attack business and personal systems every day. The number and types of cyber security threats continue to grow every day. Cyber security threats refer to possible criminal acts or attacks that attempt to legitimately access data, disrupt digital operations or damage information. These cyber threats can come from a variety of things, including corporate spies, hackers, terrorist groups, criminal organizations to employees who are dissatisfied with the company. These cyber attackers can use sensitive data belonging to individuals or companies to steal information or gain access to their financial accounts. Those are just a few examples of harmful hacker acts. That is why the role of professionals in the field of cyber security is urgently needed at this time to keep personal data protected. A cyber security expert must have an in-depth understanding of the various types of security threats on the internet, including:

a. Malware (Malicious Ware).

Malware is malicious software including viruses, worms, ransomware and spyware. The malware is activated when a user clicks on a link or attachment from an unsafe source.

b. Emotet.

The Cybersecurity and Infrastructure Security Agency (CISA) describes Emotet as an advanced modular form of Trojan development that works as a downloader or penetrates other Trojan developments. Emotet continues to be one of the most expensive and destructive pieces of malware today. Emotet spreads through e-mails, e-mail attachments, and even masquerading as one of the windows applications.

c. Denial of service (DoS)

DoS is a type of cyber attack that attacks a computer or network so that it cannot fulfill requests from users, causing the computer to not function normally or even cause damage.

d. Man In the Middle (MITM).

MITM Is a type of cyber attack, in which the hacker is in the middle of a conversation or data transmission process that occurs between the user (victim) and a website or application, without the victim knowing about it. Simply put, hackers intercept conversations and exchange data that should be confidential. Not only tapping, hackers can also disguise their identity as one of the parties involved. So as if the process of exchanging data or information occurs normally without any irregularities.

2.4 Systems Thinking

System thinking is a way of looking at something as a whole, where the parts are interconnected. Seeing as a whole means learning to understand every part involved in a system. System thinking is one of the important competencies for leaders to have. This competency allows leaders to more effectively handle and examine the complexities of both external and internal organizations, spot problems, and recognize where changes are needed.

System thinking has its basis from various sources such as the Hollis concept of Jan Smuts in

the 1920s, systems theory proposed by Ludwig von Bertalanffy in the 1940s, and cybernetics proposed by Ross Ashby in the 1950s. This field was later developed by Jay Forrester, a professor at MIT in 1956. In the book The Fifth Discipline by Peter Senge, he explained that system thinking is a pillar/basic concept of learning organization. The character of System Thinking is being able to solve difficult problems very effectively especially those involving complex problems, having a lot of feedback both internal and external and problems that are very dependent on past events or other events, so that problem solving becomes more systematic.a.

Complex, namely the interaction between elements is quite complicated.

b. Dynamic, namely the factors that change according to time.

c. Probabilistic, namely the need for a chance function in inference, conclusions and recommendations. According to Kast and James (2001), general concepts in systems science are as follows:

a. The system is comprehensive.

b. Open systems view (a relatively open system view).

c. The system receives various inputs, transforms various inputs and produces outputs in relation to the environment.

d. System boundaries (the system has boundaries).

e. Negative entropy (the system is made from a heterogeneous and sometimes negative environment).

f. The system can reach a stable position if the system is in dynamic equilibrium because negative environmental influences are minimized.

2.5 Modeling Theory.

Modellin, in general, is understood as a process of representing real objects or reality as a set of mathematical equations, graphics or charts so that it is easily understood by interested parties. More specifically, the term is often used for the process of describing the concepts that represent objects in the development of information systems. Modeling in the development of information systems, evolves in line with technological developments and development methodologies. With an object approach known as UML (Unified Modeling Language) which produces representations that can be verified through logical reasoning, testing, or even simulation.

If the model formulation is carried out, the next step will be to evaluate the system model including accuracy, availability of estimates of variables, interpretation, and validation. In this case the model formulation is always carried out based on the prevailing theories in the area where the system is located. Some of the steps that are usually carried out to carry out model formulation are from the point of view of the system and its environment. From the point of view of the level of system certainty. From the point of view of system dynamics. From the point of view of the continuity of the system. Furthermore, data processing uses the Fuzzy weighting algorithm up to level eight (Liang & Wang, 1994), Make the results of the weighting assessment of the qualitative aspect variable level. Make the results of the weighting of the assessment of the level of qualitative criteria variables. Determine the middle value of the fuzzy number (at), by adding up the values that appear at each level of the linguistic scale and then dividing the sum by the number of aspects or criteria whose values enter that level of linguistic assessment. Determine the lower limit value (ct) and upper limit value (bt) of fuzzy numbers, where the lower limit value (ct =b(i - 1)) is the same as the middle value of the level below it, while the upper limit value (bt = b (i - 1)) is the same as the middle value of the level above it.

Determining the aggregate weight of each qualitative criterion, becauseIn this study a form of

linguistic assessment was used which already had a triangular fuzzy number definition, so the aggregation process was carried out by finding the aggregate value of each lower limit value (c), middle value (a) and upper limit value (b). Look for the criterion defuzzification value, where the defuzzification method used is the centroid method. The next step is processing the defuzzification value into the final weight value for each criterion, by dividing the weight value for each defuzzification criterion by the total number of weight values for all defuzzification criteria. After implementing the Fuzzy weighting algorithm, then carry out data processing using dynamic system modelling, namely a methodology for understanding a complex problem. This methodology focuses on policymaking and how these policies determine the behavior of problems that can be dynamically modeled by systems (Richardson and Pugh 1986). The purpose of a dynamic system methodology based on a causal philosophy (cause and effect) is to gain a deep understanding of how a system works (Asyiawati, 2002, Muhammad, 2001). The stages in the system dynamic approach are:

a. Identification and definition of the problem.
b. System conceptualization.
c. Model formulation.
d. Model simulation.
e. Model verification and validation.
f. Policy analysis.
g. Policy implementation.

2.6 Research Flowchart

The stages in this research were carried out in several sequences, namely by identifying problems from several variables, followed by searching for literature sources from literature studies and from field studies that had been carried out. then carrying out data collection, identification of variables followed by carrying out processing of the data that has been obtained. To further carry out the verification and validation stages of model suitability, scenario application, and analysis so that conclusions can be obtained from the research that has been carried out

3. RESULTS AND DISCUSSION.

In this section, data analysis and research results are carried out. The data obtained is in the form of data consisting of primary and secondary data obtained by conducting direct interviews with experts from relevant agencies and also with ship journals in the field. Efforts in data collection are aimed at obtaining valid data so that it can be used according to research objectives.

3.1 Identification and Weighting of Major Cyber Warfare Threat Variables.

The purpose of identifying this variable is to deepen knowledge of the object to be studied. The identified variables are variables related to the level of threats to cyber warfare in supporting the tasks of the Indonesian Navy, then weighting is carried out in order to find the influence of the level of importance of the variable aspects and criteria.

Table 1 Identification of Main Model Variable Threats of Cyber warfare

Principal Cyber Warfare Threat Models		
No	**Variable**	**Description**
1.	Defensive Cyber Operations	Operations to protect data and information infrastructure as a matter of mission assurance.

Principal Cyber Warfare Threat Models		
No	**Variable**	**Description**
2.	Offensive Cyber Operations	Operations to penetrate systems, exploit software weaknesses, and identify security holes that allow access.
3.	Cyber Operations Intelligence	Activities and actions carried out based on a plan to achieve a routine goal in relation to space and time are carried out on the basis of orders from superiors in authority.
4.	Cyber Support	Supporting activities carried out to assist in the smooth implementation of cyber tasks and missions.

After the identification of the influential variables in the cyber warfare threat model is carried out, then the research is continued by looking for the weight of the influence of the importance level of the aspect variables and criteria. The initial stage in the preparation of the model is the identification and data collection of the main aspect variables that influence the threat of cyber warfare obtained from previous research references and the results of Depth Interview interviews with experts. The purpose of identifying this aspect variable is to sharpen the researcher in processing and compiling the model to be studied which will later be used as a constant in the System Dynamic modeling formulation to determine values.

E1 : Expert 1
E2 : Expert 2
E3 : Expert 3
E4 : Expert 4
E5 : Expert 5

Table 2 Aggregated Assessment Criteria for Defensive Cyber Ops Aspects.

NO	**CRITERIA**	**E1**	**E2**	**E3**	**E4**	**E5**
1	Monitoring	8	9	9	9	9
2	Observation	8	8	7	7	7
3	Identification	8	8	9	9	9
4	Protection	8	5	8	6	7
5	Mitigation	9	8	8	9	8
6	Investigation	8	9	9	9	8
7	Countermeasures	9	9	9	7	9
8	Recovery	8	7	8	9	8

Table 3 Aggregated Assessment Criteria for Aspects of Offensive Cyber Ops.

NO	**CRITERIA**	**E1**	**E2**	**E3**	**E4**	**E5**
1	Exploitation	8	9	9	9	9
2	Forensics	8	8	6	8	8
3	Counter Exploitation	9	9	9	8	8
4	Information and Network Attacks	9	4	7	8	7

Table 4 Aggregate Criteria Assessment Aspects of Support Cyber.

NO	CRITERIA	E1	E2	E3	E4	E5
1	Development Planning	9	9	9	9	9
2	System Development	7	7	8	8	8
3	Cyber Certification	8	8	9	9	9
4	Implementation of Training	8	5	7	7	5
5	Cyber Workshops	8	9	9	9	9
6	Operations Support	8	7	9	8	9

Table 5 Aggregated Assessment of Cyber Ops Intelligence Aspect Criteria.

NO	CRITERIA	E1	E2	E3	E4	E5
A	**TACTICAL**					
1	Security Operation Center/SOC	9	9	8	9	8
2	Security Information Event Management/SIEM	9	9	8	9	9
3	Firewalls	8	8	9	8	9
4	End Points	9	9	9	8	8
5	Instruction Detection System/IDS & Instruction Prevention System/IPS)	7	9	8	7	8
B	**OPERATIONAL**					
1	Threat Hunter	9	8	7	9	9
2	SOC Analysist	8	9	9	9	8
3	Vulnerability Management	8	9	8	8	8
4	Incident Responses	9	8	9	9	9
5	Insider Threat	9	9	9	8	8
C	**STRATEGIC**					
1	Chief Information Security Officer/CISO	8	9	9	8	9
2	Chief Information Officer/CIO	8	9	9	8	9
3	Chief Technology Officer/CTO	9	9	9	8	8
4	Executive Board	9	8	8	9	9
5	Strategic Intelligence	9	9	9	8	9

Table 6 Main Aspect Weighting Value.

NO	MAIN ASPECT	FINAL WEIGHT
1	The aspect of Defensive Cyber Operation	0.27

2	Offensive Aspects Of Cyber Operation	0.24
3	Aspect Of Cyber Support	0.25
4	Intelligence Aspect Of Cyber Operation	0.24

Table 7 Defensive Cyber Ops Aspect Weighted Values

NO	CRITERIA	FINAL WEIGHT
1	Monitoring	0.1391
2	Observation	0.0774
3	Identification	0.1273
4	Protection	0.1229
5	Mitigation	0.0998
6	Investigation	0.1523
7	Countermeasures	0.1246
8	Recovery	0.1567

Table 8 Offensive Cyber Ops Aspect Weighted Values

NO	CRITERIA	FINAL WEIGHT
1	Exploitation	0.292
2	Forensics	0.260
3	Counter Exploitation	0.208
4	Information and Network Attacks	0.240

Table 9 Aspect Weighting Value of Cyber Support.

NO	CRITERIA	FINAL WEIGHT
1	Development Planning	0.1051
2	System Development	0.1669
3	Cyber Certification	0.1729
4	Implementation of Training	0.2068
5	Cyber Workshops	0.1356
6	Operations Support	0.2128

Table 10 Aspect Weighting Value of Cyber Ops Intelligence.

NO	CRITERIA	FINAL WEIGHT
A	**tactical**	

NO	CRITERIA	FINAL WEIGHT
1	Security Operation Center/SOC	0.0396
2	Security Information Event Management/SIEM	0.0651
3	Firewalls	0.1669
4	End Points	0.0511
5	Instruction Detection System/IDS & Instruction Prevention System/IPS)	0.0779
B	**OPERATIONAL**	
1	Threat Hunter	0.0779
2	SOC Analysist	0.0637
3	Vulnerability Management	0.0801
4	Incident Responses	0.0511
5	Insider Threat	0.0779
C	**STRATEGIC**	
1	Chief Information Security Officer/CISO	0.0511
2	Chief Information Officer/CIO	0.0779
3	Chief Technology Officer/CTO	0.0637
4	Executive Board	0.0801
5	Strategic Intelligence	0.0801

3.2 Main Concept of a Threat Model.

The causal loop model is made to show the variables described in the model, in this case, it has been compiled based on the initial variables that have been identified.

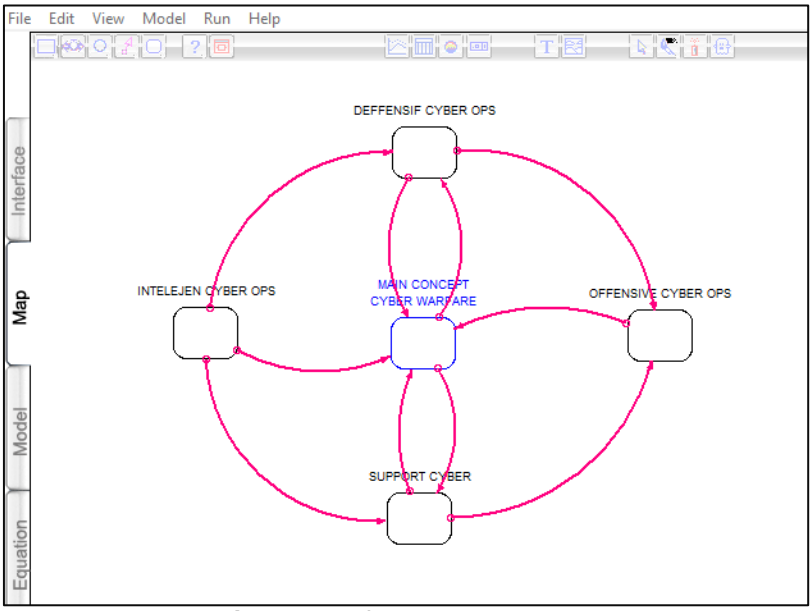

Figure 1 Main Concept

Figure 3.1 is the structuralization of models and systems that occur in the cyber warfare threat model system. From the conceptualization of the causal loop diagram model above, it can be seen that the cyber warfare threat system is influenced by the development of system dynamics from 4 (four) variables, namely Defensive Cyber Operation, Offensive Cyber Operation, Intelligence Cyber Operation, and Cyber Support.

CONCLUSION.

After carrying out the entire data processing process in working on the thesis, conclusions can be made based on the results of data analysis and discussion that have been carried out. There are 4 (four) main variables of the cyber warfare threat model, namely Defensive Cyber Ops, Offensive Cyber Ops, Espionage Cyber Ops, and Cyber Support. Where each variable influences the other on threats so that this can be implemented as a consideration for the leadership of the Indonesian Navy in making decisions.

ACKNOWLEDGEMENTS

The researcher would like to thank the Sttal Commander and all staff who have provided assistance, direction, and instructions in completing the making of this pepper.

REFERENCES

Ahmed, MS, & Daim, MK (2020) The Inevitable Battleground for Competing Powers: Cyberwarfare.

Bobbio, A., Campanile, L., Gribaudo, M., Iacono, M., Marulli, F., & Mastroianni, M. (2022). A cyber war perspective on the risks associated with IoT devices health and contact tracing. Neural Computing and Applications.

Cimbala, Stephen J. (2022) "Nuclear-Crisis Management and Cyber War A Dangerous Crossroads, Naval War College Review Vol. 75.

C. Rohith and RS Batth. (2019) "Cyber Warfare: Nations Cyber Conflicts, Cyber Cold War Between Nations and its Repercussion," 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE).

Craigen, D., Daikun-Thibault, N., Purse, R., 2014. 'Defining Cybersecurity'. Technology Innovation Management Reviews.

Davis, EVW (2021). Shadow Warfare: Cyberwar Policy in the United States, Russia, and China. Rowman & Littlefield Publishers.

Datta, P. (2021). Hannibal at the Gates: Cyberwarfare & the Solarwinds sunburst hack. Journal of Information Technology Teaching Cases.

Ebert, H., Maurer, T., 2017. International Relations and Cyber Security: Carnegie Contribution to Oxford Bibliographies.

Eun, YS, & Aßmann, JS (2016). Cyberwar: Taking stock of security and warfare in the digital age. International Studies Perspectives.

Hodgson, Q., et.al., 2019. 'Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace, Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace.

James J. Wirtz. (2018) The Cyber Pearl Harbor redux: helpful analogy or cyber hype Intelligence and National Security.