INTERNATIONAL JOURNAL OF SOCIAL AND MANAGEMENT STUDIES (IJOSMAS)

Vol. 4 No.4 https://www.ijosmas.org e-ISSN: 2775-0809

Implementation of Information Technology for the Indonesian Navy in Dealing with Cyber Threats

Zainal Syahlan[1*]
[1]Politeknik Angkatan Laut
Ciledug Raya Street No.2, Seskoal, South Jakarta, Indonesia 12230
*Corresponding Author: zsyahlan@gmail.com

Abstract *- National defence in the seas faces increasingly complex challenges due to developments in information technology. Cyber threats are a significant threat to national security, including in the context of national defence at sea. Therefore, the Indonesian Navy as a component of national defence needs to apply sophisticated information technology to deal with this threat. This study aims to analyse the application of Indonesian Navy information technology in dealing with cyber threats to support national defence at sea. The method used in this study is a qualitative method with a case study approach. This research involved collecting data through in-depth interviews, participant observation, and analysis of related documents. The results of this study indicate that the Indonesian Navy has implemented various innovative information technologies to deal with cyber threats. The application of this information technology involves Information Technology Infrastructure (hardware), the readiness of the Required Cyber Operation Software and Human Resources (brain ware), as well as the development of cyber capabilities within the organization. Through the application of this information technology, the Indonesian Navy can support national defence at sea more effectively*

Keywords*: Technology, Indonesian Navy, cyber threats, national defence.*

I. INTRODUCTION

In an era of growing globalization, information technology plays a very important role in almost every aspect of our lives. The application of information technology has brought about profound changes in the way we work, communicate, learn, and interact with the world around us.[1][2] The application of information technology includes the use of hardware, software, computer networks and various applications that enable the efficient processing, storage, retrieval and exchange of information.[3] Information technology provides the ability to automate processes, increase productivity, expand access to information, and connect people from different geographic locations.[4] In this case the application of information technology involves the implementation and integration of information systems designed to meet the needs and goals of the organization. Organizations across a wide range of sectors, including business, education, government, healthcare and others, rely on information technology to improve operational efficiency, improve service quality and achieve competitive advantage.[5] The application of information technology has also changed the way we interact with society and access information. In the digital era, we can easily connect with people around the world through social media platforms, email and instant messaging applications. Information that was previously difficult to access is now available in seconds via the internet. However, the application of information technology also poses certain challenges and risks. Data security, privacy and information leakage are important issues that need to be addressed. In addition, the adoption of information technology can also create a digital divide, where some people can be left behind in keeping up with technological developments.[6]

Along with the current developments in various fields of human life, when talking about National defence, the meaning and context it faces, of course, also evolves. Along with the development of science and technology, of course this has a positive value for the ease of human life, but of course this also carries the potential to harm humans. In the context of the State and defence the development of Information Technology is followed by potential threats in the field of cyber security to the state.[7] According to the results of a survey conducted by the Association of Indonesian Internet Service Providers (APJII) in the 2022-2023 period, internet users in Indonesia reached 215.63 million people. This figure shows an increase of 2.67% compared to the

previous period, where there were 210.03 million internet users. This data confirms that the internet is increasingly penetrating various layers of Indonesian society.[8][9] It can be said that in Indonesia there is quite high digital penetration, currently all people in this country depend quite heavily on technology. This dependence is not only experienced by ordinary people, but the government and state affairs are also dependent on technology. Therefore security in the use of technology is quite important because the potential for cyber-crime is increasingly open with the massive use of technology today. Currently, Information Technology is not only used in the industrial or economic fields, but also in the defence and security sector of a country. [10] The use of information technology for military purposes has grown rapidly in various countries, especially for the interests of national defence, among others being used in information systems and data processing, command and control systems, and weapons control systems for defence purposes.

Implementation of information support operations can be in the form of Cyber Security and Security Awareness. In practice, the Indonesian Navy still has obstacles, including: Information Technology infrastructure that is owned is not optimal, cyber operation software is still limited and Human Resources as crew members still need to be improved and interoperability between cyber stakeholders has not been maximized. Advances in technology and information will certainly pose a new threat in cyber space, namely cyber-crime.[11][12] Cybercrime is a crime that was born as a negative impact from the development of applications on the internet.[13] In analysing the impact of cyber-crime on a country's defence, it is necessary to identify risk management that can determine how big the probability and consequences of cyber-crime are. The risks faced in overcoming the threat of cyber-crime are not inferior to conventional warfare. This causes the identified risks to be able to produce a national defence strategy in dealing with cybercrime threats.[14] The Indonesian Navy needs to develop and optimize Information Technology in an effort to improve performance to support national defence at sea. Good infrastructure, systems and management are needed as well as the integration of all information systems that are able to adapt to very fast technological changes so as to provide maximum benefits for the advancement of the Indonesian Navy, especially in dealing with cyber threats which are currently increasingly prevalent.

II. METHOD

In this study using descriptive qualitative which aims to understand and describe the phenomenon studied in detail, by exploring the perspectives, attitudes, and beliefs of individuals or groups involved in research. This study does not aim to test hypotheses or make statistical generalizations, but rather focuses on an in-depth understanding of the context and complexity of the observed phenomena. This method focuses on explanations and interpretations from the perspective of research participants. Qualitative descriptive research generally uses a qualitative approach in data collection and analysis.[15][16] Data collection methods that are often used include interviews, participant observation, document studies, and focus group discussions. The data obtained is then analysed thematically, by looking for patterns, themes, or categories that emerge from the collected data. After that the researcher determines the topic or research problem that he wants to examine descriptively. Next, the researcher will design a research design, including participant selection, data collection techniques, and data analysis procedures. Data analysis in qualitative descriptive research using SWOT analysis will be used as a framework for understanding certain situations or phenomena holistically.[17][18] Through the identification of strengths, weaknesses, opportunities and threats from the data collected. Researchers try to understand the meaning contained in the data and describe it in a rich and deep narrative. Research conclusions focus on understanding the context of the phenomenon studied, by describing the characteristics, patterns, or findings that emerge from the data analysis.

III. RESULT AND DISCUSSION

The technical supervisor of computer technology within the Indonesian Navy is the Information and Data Processing Service of the Indonesian Navy which has an important role regarding the use of Information Technology and computers within the Indonesian Navy. The Data Centre owned is a data centre for the Indonesian Navy which is able to guarantee the availability of services for all information systems and databases from various risks. The data centre is also a place for all computer servers and also as a Disaster Recovery Centre Server unit under it. In ensuring network security, the Indonesian Navy has a Network System Security Laboratory which functions to improve network system security capabilities and is responsible for network system security and information systems in the Indonesian Navy. The security of the network system is not only shown in the internal network but in the overall relationship between inter and interconnection between units,

command and control centres and the smallest elements of the Indonesian Navy in the field such as the Indonesian Republic Ship and the Task Force.

A. Optimal Indonesian Navy Information Technology Infrastructure

Reliable information technology infrastructure is one of the important pillars in cyber defence. This includes hardware, communications networks, and applicable policies and procedures. The Indonesian Navy needs to ensure that the equipment and systems they use can identify, address and respond to cyber-attacks quickly and effectively. One of the main components of information technology infrastructure is a security system. The Indonesian Navy must have a strong layer of defence to protect their sensitive data, operational systems and communication networks from possible attacks. This involves the use of firewalls, data encryption, intrusion detection systems, and strict policies and procedures for managing information access and use. In addition, it is also important for the Indonesian Navy to have a well-trained and qualified cyber security team. This team will be responsible for monitoring and protecting their systems, as well as responding quickly to detected attacks. They also need to stay abreast of information technology developments and the latest cyber-attack trends to be able to build an effective defence. In dealing with cyber threats, the Indonesian Navy can also take advantage of cooperation with other parties, both on a national and international scale. This collaboration can involve exchanging information, training, and cooperation in the development of cyber defence technologies and strategies. With a strong information technology infrastructure, the Indonesian Navy will have better capabilities in dealing with increasingly complex cyber threats. With strong protection of their systems, the Indonesian Navy can ensure operational continuity, maintain the security and integrity of sensitive data, and make a significant contribution to maintaining Indonesia's maritime sovereignty.

B. Required Cyber Operations Software Readiness

Cyber operations software refers to the various applications, systems and protocols used to manage, protect and monitor the security of computer networks and IT infrastructure within the Indonesian Navy's operational environment. This includes security policies, intrusion detection, data security, risk management, and cyber disaster recovery. The cyber threats faced by the Indonesian Navy are very diverse and continue to evolve along with advances in technology. Some of the threats that need to be confronted include hacking attacks, malware attacks, DDoS (Distributed Denial of Service) attacks, ransom ware attacks, and other threats aimed at accessing, stealing, or destroying sensitive information and vital infrastructure. To deal with these threats, the readiness of cyber operation software is very important. Reliable and sophisticated software can provide effective protection against cyber-attacks, detect suspicious activity, and respond quickly to reduce the impact that may arise. In addition, good cyber operations software must also be able to continuously monitor networks and systems, analyse and report detected threats, and provide timely solutions to address security incidents. In the context of the Indonesian Navy, the required cyber operations software must be specifically designed for their needs. This includes developing adequate systems to secure data and communications, protect weapons systems, and carry out effective and coordinated cyber operations. In this review, it will be discussed further regarding various aspects of cyber operations software required by the Indonesian Navy to deal with expected cyber threats. This includes strong security policies, intrusion detection systems, data security technologies, risk management, and an effective cyber disaster recovery plan**.**

C. Optimal Indonesian Navy Human Resources (Brain ware)

In dealing with this cyber threat, the Indonesian Navy realizes that optimal human resources or "brain ware" is a key factor in securing their infrastructure and data. Cyber threats evolve rapidly and are increasingly complex, involving attacks such as hacking, malware attacks, DDoS attacks, and phishing attacks that aim to steal sensitive information or damage systems. As information technology advances, attackers are becoming more sophisticated and able to change their tactics constantly. Therefore, the Indonesian Navy realizes the importance of having skilled and well-trained human resources in dealing with this threat. Optimal human resources in this context refer to personnel who have in-depth knowledge, skills and understanding of cyber security and information technology. They must be able to identify threats, track attacks as they occur, and take appropriate actions to address and recover affected systems. In addition, they must also be able to develop an effective security strategy, carry out risk assessments, and engage in proactive security practices. The Indonesian Navy recognizes that investing in optimal human resource development in terms of cyber security is a must. Continuous training and education is an important part of this strategy. Indonesian Navy personnel need to be kept updated with the latest developments in security technology and attack tactics used by attackers. In addition, collaboration with other institutions and organizations that have expertise in cyber security is also important to gain insight and a broader

understanding of existing threats. In this introduction, we will explore how the Indonesian Navy can achieve optimal human resources in dealing with cyber threats. We will see the efforts being made to increase the knowledge, skills and understanding of personnel in terms of cyber security. In addition, it will also discuss the importance of collaboration and cooperation with external parties in order to strengthen the Navy's cyber defence. With increased awareness of the importance of optimal human resources, the Indonesian Navy can be more prepared and responsive in dealing with ever-evolving cyber threats**.**

D. Established Interoperability between Stakeholders

The level of Information Technology capability in dealing with cyber threats must be carried out in all regions of Indonesia. This means that there must be interoperability of capabilities between stakeholders in dealing with cyber threats as the main controlling command, but in the deployment of forces a tactical command must be formed. In fact, cyber capabilities must also be placed in operational units, in order to be able to protect every electronic data in every unit, force, or other military technical agency. Interoperability between Stakeholders is expected to be able to protect various websites, websites and communication networks owned by the government, state agencies, and various ministries from various cyber attacks that often occur without the awareness of various parties. Institutions and other related agencies must work hand in hand in empowering the potential of cyber space and digital potential that they have, as artificial resources, to be empowered in stemming and dealing with cyber wars. The government must carry out various inventories, identify, foster, and manage various cyber power potentials that Indonesia has, especially social media users, the public, and various information communities. Cyber communication to synergize with each other in facing cyber threats

E. Contribution

1) The optimal application of Indonesian Navy Information Technology will be able to deal with today's rapidly developing cyber threats: The development of Information and Communication Technology is of course adding to the trend of world technological development with all forms of human creativity. The development of this technology is increasingly expanding into various fields, where people can quickly get the information they need at any time. Nearly a third of the world's population uses the internet in their daily lives, including the Indonesian Navy. With the mastery of knowledge caused by advances in the field of Information Technology, the enemy can be brought to its knees by means of computer technology. For example the use of artificial intelligence programs to simulate enemy formations and forces allows attacks to be effective with a fairly high success rate. The rapid development of Information Technology has also made it possible for the formation of new military units, whose activities are related to the process of collecting, processing and disseminating information. Information security is a set of methodologies, practices or processes designed and implemented to protect personal information or data from unauthorized access, use, misuse, interference or modification. Information security aims to protect data at various stages, whether in the process of storing, transferring or using it. With an information security system or what is known as optimal cyber security, of course, you will be able to deal with cyber threats that are rapidly increasing in various aspects. The Indonesian Navy must be able to build its Information Technology that is integrated, tough and integrated in dealing with future cyber threats
2) Realization of National defence at sea: The Indonesian Navy, in carrying out its duties optimally, requires the main tools of modern weapons systems based on the latest technology along with reliable operational support systems and equipment and also based on the latest technology with high operational readiness. Therefore the defence sector in Indonesia and special institutions to deal with defence only focus on preparing to face physical threats. In this case, of course, it can be seen from the skill or skills of the Human Resources that are in it are only focused on having the abilities for physical warfare/threats. From another perspective, such as the facilities and infrastructure in the form of weapons that are owned are for the benefit of physical attacks. This then needs to be paid more attention to considering the threat sector that is currently expanding in the cyber sector due to technological advances, the concept of national defence at sea.

F. Indicator of Success

1) Well Addressed Cyber Threats: In cyber threats, there are methods of attack which are certainly different from classic wars, conventional wars or other physical wars. The domain of Cyber Warfare is in cyberspace, where the attacker is an Information Technology expert who does not have to come directly to the country being attacked. The area that is attacked is also not a physical area, territorial area, or geographical area, but a cyber-area. Three main reasons why a computer or communication system becomes the target of an opponent's cyber operations, namely: the system contains crucial information;

the system is related to important officials or influential people; and the system affects the basic needs of society. One of the operational support systems that is very necessary is an information system that is integrated and able to manage data and information quickly, precisely, accurately, and safely. An information system capable of presenting information in a comprehensive, real time and online manner in the context of organizational development and implementation of control, deployment and operation of sea power as well as in dealing with the dynamics of information development related to cyber threats in the Indonesian Navy can be handled properly.

2) Realization of National defence at Sea: the government has defence institutions to maintain security from potential attacks. One of the institutions formed by the government regarding defence affairs is the Indonesian National Armed Forces. However, the Indonesian National Armed Forces itself was formed as a government agency engaged in the defence sector which in this regard focuses on the potential for physical attacks. In general, when talking about state security it is synonymous with security from potential physical threats. Therefore the defence sector in Indonesia and special institutions to deal with defence only focus on preparing to face physical threats. In this case, of course, it can be seen from the skill or skills of the Human Resources that are in it are only focused on having the abilities for physical warfare/threats. From another perspective, such as the facilities and infrastructure in the form of weapons that are owned are for the benefit of physical attacks. This then needs to be paid more attention to considering the threat sector that is currently expanding in the cyber sector due to technological advances, the concept of national defence at sea.

G. Solution to problem

The potential for attacks on the cyber sector is currently occurring both throughout the world and in Indonesia itself is currently increasingly massive. Cyber-attacks themselves are of various types when viewed from the perpetrators and also their goals. Cyber-attacks can be carried out by individuals or even at the organizational or corporate level, maybe even at the country level. While the goals are also very diverse, from trivial goals such as curiosity from individuals or even to very serious goals such as espionage or sabotage in a more macro scope such as state information. Cyber-attacks in quantity are currently very massive followed by potential losses that are quite large if the targets also vary from harmless to very dangerous in the field of national defence. If viewed from a macro perspective, namely national defence, cyber attacks are of course a fairly serious threat. The use of technology, especially the internet, has now penetrated all sectors of human life, including the government sector. Assets in the form of digital information are things that have the potential to be taken and misused by other parties. Therefore it is very important for the state to have the capability and system to prevent cyber-attacks in the efforts of national defence. The Indonesian National Armed Forces as the front guard institution in the national defence structure, ideally also has the ability to be able to expand the scope of the focus of preparation in national defence efforts.

1) Policy

The application of Information Technology for the Indonesian Navy to deal with cyber threats in order to support the State's defence at sea, requires the implementation of the formulation of a policy to increase the optimal application of Information Technology. Policies are prepared based on current conditions and problems encountered in the Indonesian Navy. However, with the existence of factors that influence both internal factors and external factors which are always dynamic, opportunities and constraints are inevitable in achieving the desired goals. These opportunities and constraints must be utilized as well as possible in order to achieve the desired goal, namely to deal with cyber threats in the framework of supporting the State's defence at sea. The policies set are:

2) Strategy

Based on the above policies, it needs to be translated into an appropriate strategy so that it becomes a reference or basis in determining the efforts to be made. These strategies as a follow-up to the policies that have been formulated, are realized through a step or way (ways) supported by means and infrastructure (means) in order to achieve targets (ends) through setting priority scales for the targets to be achieved. As for determining the strategy in optimizing the application of Information Technology in the Indonesian Navy to deal with cyber threats in order to support the State's defence at sea. In this writing how to determine the strategy using the SWOT method approach (Strengths, Weaknesses, Opportunities, and Threats). Where the initial step of this strategy is to determine the internal and external factors in table 1 and figure1:

Table 1. Recapitulation of the results of SWOT weights and ratings

Internal Factors Analysis Summary (IFAS)	Weight	Scores	Weight x Scores
Strength			
Conditions of the State Revenue and Expenditure Budget	0,16	3,50	0,56
Domestic industry	0,15	3,00	0,45
Integrated Human Resources	0,15	3,75	0,56
Application of Information Technology	0,15	3,50	0,53
Amount			2,10
Weakness			
Infrastructure is still lacking	0,12	3,75	0,44
Suboptimal software	0,12	3,50	0,41
Limited Human Resources	0,14	3,25	0,46
Sectorial ego mindset	0,13	3,25	0,41
Amount			1,73
S - W			0,37

External Factors Analysis Summary (EFAS)	Weight	Scores	Weight x Scores
Opportunities			
IT development trends	0,17	3,00	0,51
Simplify operations	0,16	2,50	0,40
Create independence	0,16	2,75	0,44
Stakeholder cooperation	0,16	3,25	0,52
Amount			1,87
Threats			
Global cyber threat	0,12	2,75	0,32
Cyber threat protection	0,10	3,00	0,30
Sectorial ego occurs	0,10	3,25	0,33
Internal threats to human resources	0,11	3,25	0,36
Amount			1,31
O - T			0,56

S

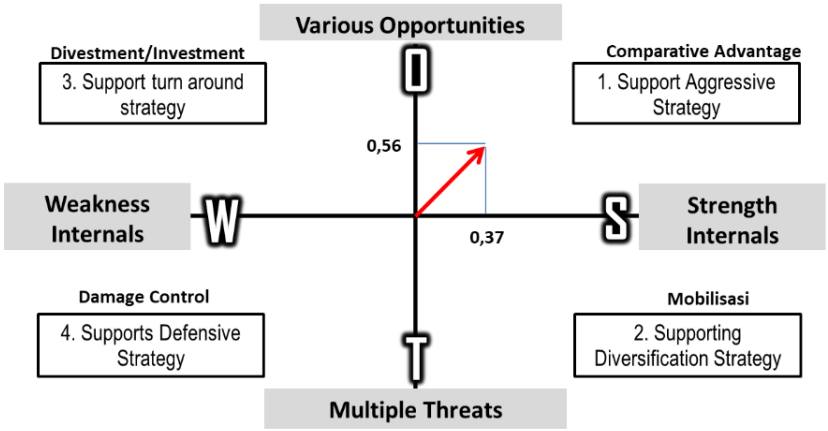

Figure 1. Quadrant SWOT

a) Strategy 1: Supporting the development and procurement policy directions for the Indonesian Navy Information Technology as needed, the strategy developed is to prepare the Navy Information Technology infrastructure in stages and continuously in accordance with the established roadmap, through coordination and development of Information Technology infrastructure related to cyber security.
b) Strategy 2: Supporting the direction of software improvement and development policies in supporting the Navy's cyber operations, namely by fulfilling the Navy's cyber operation software prioritizing the domestic industry as a whole and evenly in every operational unit of the Indonesian Navy.
c) Strategy 3: Supporting the policy directions for developing human resources who have integrity and competence in the field of Information Technology, by continuously preparing Indonesian Navy human resources through education, training, quality development programs.
d) Strategy 4: Supporting the policy direction of increasing interoperability between Information Technology stakeholders in dealing with rapidly growing cyber threats, through training programs, cooperation and regulations that bind related parties.

3) Effort: In order to realize and implement the above strategies, it is necessary to have positive efforts as elaboration and concrete actions, as follows:

a) Strategy Effort-1.

The Indonesian Navy coordinates with the Ministry of Defence and the Indonesian National Armed Forces regarding the procurement and development of information technology infrastructure that will be carried out so that the infrastructure can be built according to the expected needs; In sustainable infrastructure development, the Government through related agencies cooperates with foreign Information Technology industries in carrying out Technology Transfers so that the capabilities of the domestic industry increase; To determine hardware standards to be used, the Indonesian Navy can form a special team that is expert in Information Technology by involving consultants who are experts, qualified and have integrity to determine hardware standards to be used within the Indonesian Navy; The Indonesian Navy allocates a budget for the installation of Wi-Fi/VSAT satellite infrastructure throughout KRI. This installation is expected to provide interoperability between staff on land and KRI elements carrying out operations at sea; in the framework of the independence and security of the national internet network, the Government is currently reviewing and planning to have its own national satellite managed by the government. So that internet network security can be controlled for its use and security, especially in the field of defence; To improve capabilities in carrying out cyber operations, the Indonesian Navy needs to issue a budget plan policy to meet the needs of the operational network of the Indonesian Navy's work units that do not yet have or improve cyber operations capabilities.

b) Strategy Effort-2

The government issues regulations regarding the use of Information Technology software by prioritizing domestic products for the benefit of national defence so as to ensure security; The Indonesian Navy makes regulations regarding software standards that are installed on hardware devices. To determine standards for the Indonesian Navy, it is necessary to coordinate with the Ministry of defence and other forces; The Indonesian Navy needs to take policy steps to develop domestic product software. Steps that can be taken are to increase the role of Naval research and development service in collaboration with universities that are competent in the field of Information Technology in research and development; The Indonesian Navy issues regulations on network security related to the use of Information Technology software and fulfils standard software requirements in operational units of the Indonesian Navy in carrying out cyber protection and operations as needed; The Network Security System Laboratory, which is in the process of being validated to become a Cyber Unit of the Indonesian Navy, carries out socialization on the use and training of cyber program software to all operational units so that misunderstandings, data misuse and data leakage occur due to the lack of vigilance of crew personnel in the field.

c) Strategy Effort-3

The Indonesian Navy fulfils the needs of human resources who have competence in the field of Information Technology according to organizational needs; In carrying out the recruitment of human resources in the Information Technology sector, they must pass a mental readiness test through a psychological test so that they match the profile of Human Resources for cyber defence, such as: must be able to work under stressful conditions, have high integrity, be disciplined, have learning abilities and so on. -other, in accordance with established standards; Training and capacity building

for HR can be carried out by means of: promotion/awareness raising programs for all Information Technology stakeholders and increasing knowledge/skills through in-class, on the job, online training programs and their combinations; Increased knowledge and skills in handling cyber security that must be owned include at least in the fields of digital forensics, incident response, operating systems, data communication networks, penetration testing, web/online based applications, conformity testing, network security, digital control systems and cyber security knowledge other; The Indonesian Navy carries out communication security outreach to every soldier so that awareness of network and information security can be maintained.

d) Strategy Effort-4

The government issues regulations regarding the role of interoperability between related Information Technology stakeholders in dealing with cyber threats, so as to create integration; The Ministry of Communication and Informatics, the National Cyber and Crypto Agency, the Ministry of Defence, the Indonesian National Armed Forces and the Navy are increasing cooperation in the field of Information Technology to deal with increasing cyber threats through data and information sharing; Handling the threat of cyber-attacks cannot be carried out partially, but requires comprehensive, integral and integrated handling steps between relevant stakeholders; The Ministry of Defence together with institutions, parties and other related agencies must work hand in hand in empowering the potential of Information Technology and its cyber warfare, one unified view and one perception to synergize one action, one policy and one complete action plan; The Indonesian Navy makes regulations regarding software standards that are installed on hardware devices with the aim of realizing interoperability between stakeholders in the future..

IV. CONCLUSION

In dealing with increasingly complex cyber threats, the Indonesian Navy needs to ensure that the equipment and systems it uses can identify, overcome and respond to attacks quickly and effectively. This involves the use of security systems that include firewalls, data encryption, and intrusion detection systems, as well as strict policies and procedures to manage access to and use of information. In addition, it is important for the Indonesian Navy to have a well-trained and qualified cyber security team. This team is responsible for monitoring and protecting systems, as well as responding quickly to detected attacks.

A good cyber operations software must be capable of continuous monitoring of networks and systems, analyse and report on detected threats, and provide timely solutions to resolve security incidents. In the context of the Indonesian Navy, this software must be specifically designed to meet their needs, including securing data and communications, protecting weapons systems, and conducting effective and coordinated cyber operations. By implementing the right cyber operations software, the Indonesian Navy can increase its readiness to deal with evolving cyber threats and minimize the possible impact of cyber-attacks.

The Indonesian Navy realizes the importance of having optimal human resources in dealing with increasingly growing and complex cyber threats. Continuing training and education is an important part of this strategy, to keep personnel updated with developments in security technology and attack tactics used by attackers. With increased awareness of the importance of optimal human resources, the Indonesian Navy will be more prepared and responsive in dealing with ever-evolving cyber threats. In an era filled with cyber threats, security and protection of infrastructure and data is a top priority, and skilled and trained human resources are a key factor in achieving this goal.

Capability interoperability, close cooperation and collaboration between all stakeholders in the field of Information Technology and cyber security are needed to empower the potential of cyberspace and digital as a resource that can be used to fight cyber-attacks. Thus, Indonesia can strengthen cyber defence and be able to deal with cyber threats that may arise in the future.

REFERENCES

[1] L. Mengcheng and T. Tuure, “Information Technology–Supported value Co-Creation and Co-Destruction via social interaction and resource integration in service systems,” *J. Strateg. Inf. Syst.*, vol. 31, no. 2, p. 101719, 2022, doi: 10.1016/j.jsis.2022.101719.

[2] P. Putra Tampi, S. Diana Nabella, and D. P. Sari, “The Influence of Information Technology Users, Employee Empowerment, and Work Culture on Employee Performance at the Ministry of Law and Human Rights Regional Office of Riau Islands,” *Enrich. J. Manag.*, vol. 12, no. 2, pp. 1620–1628,

2022.

[3] K. Razikin and B. Soewito, "Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework," *Egypt. Informatics J.*, vol. 23, no. 3, pp. 383–404, 2022, doi: 10.1016/j.eij.2022.03.001.

[4] B. Alhayani, S. T. Abbas, D. Z. Khutar, and H. J. Mohammed, "Best ways computation intelligent of face cyber attacks," *Mater. Today Proc.*, no. xxxx, 2021, doi: 10.1016/j.matpr.2021.02.557.

[5] E. Tariq, M. Alshurideh, I. Akour, and S. Al-Hawary, "The effect of digital marketing capabilities on organizational ambidexterity of the information technology sector," *Int. J. Data Netw. Sci.*, vol. 6, no. 2, pp. 401–408, 2022, doi: 10.5267/j.ijdns.2021.12.014.

[6] P. T, S. P. Djati, and E. Tanti P., "The Effect of Digital Leadership, organizational culture, digital competence and organization's commitment on Organizational Performance: Information Technology System in Indonesian Navy," *Int. J. Sci. Res. Manag.*, vol. 11, no. 04, pp. 4833–4846, 2023, doi: 10.18535/ijsrm/v11i04.em06.

[7] D. I. Sensuse, P. A. W. Putro, R. Rachmawati, and W. D. Sunindyo, "Initial Cybersecurity Framework in the New Capital City of Indonesia: Factors, Objectives, and Technology," *Inf.*, vol. 13, no. 12, pp. 1–10, 2022, doi: 10.3390/info13120580.

[8] M. Boeding, K. Boswell, M. Hempel, H. Sharif, and J. Lopez, "Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid †," vol. 15, no. 1, pp. 1–22, 2022, doi: https://doi.org/10.3390/en15228692.

[9] T. Sobb, B. Turnbull, and N. Moustafa, "Supply chain 4.0: A survey of cyber security challenges, solutions and future directions," *Electron.*, vol. 9, no. 11, pp. 1–31, 2020, doi: 10.3390/electronics9111864.

[10] E. Ukwandu *et al.*, "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends," *Inf.*, vol. 13, no. 3, pp. 1–22, 2022, doi: 10.3390/info13030146.

[11] M. H. Alqaraleh, M. O. S. Almari, B. J. A. Ali, and M. S. Oudat, "the Mediating Role of Organizational Culture on the Relationship Between Information Technology and Internal Audit Effectiveness," *Corp. Gov. Organ. Behav. Rev.*, vol. 6, no. 1, pp. 8–18, 2022, doi: 10.22495/cgobrv6i1p1.

[12] P. A. Ahmad, "Cyber Security Is More than Just a Question of Information Technology," *J. Image Process. Intell. Remote Sens.*, no. 12, pp. 1–7, 2021, doi: 10.55529/jipirs12.1.7.

[13] A. M. Bossler and T. Berenblum, "Introduction: new directions in cybercrime research," *J. Crime Justice*, vol. 42, no. 5, pp. 495–499, 2019, doi: 10.1080/0735648X.2019.1692426.

[14] R. Desiana and S. C. Prima, "Cyber security policy in Indonesian shipping safety," *J. Marit. Stud. Natl. Integr.*, vol. 5, no. 2, pp. 109–117, 2022, doi: 10.14710/jmsni.v5i2.13673.

[15] C. McMullin, "Transcription and Qualitative Methods: Implications for Third Sector Research," *Voluntas*, vol. 34, no. 1, pp. 140–153, 2023, doi: 10.1007/s11266-021-00400-3.

[16] A. B. Ferial, Mattalatta, and H. Tamsah, "Pengaruh Kompetensi Terhadap Kinerja Melalui Motivasi Dan Disiplin Tutor Pada Program Pendidikan Luar Sekolah Pada Pusat Kegiatan Belajar Masyarakat (PKBM) Kota Makassar," *YUME J. Manag.*, vol. 2, no. 1, 2019, [Online]. Available: https://journal.stieamkop.ac.id/index.php/yume/article/view/352

[17] M. A. Benzaghta, A. Elwalda, M. Mousa, I. Erkan, and M. Rahman, "SWOT analysis applications: An integrative literature review," *J. Glob. Bus. Insights*, vol. 6, no. 1, pp. 55–73, 2021, doi: 10.5038/2640-6489.6.1.1148.

[18] A. Citra Birru, S. Sudarmiatin, and A. Hermawan, "Competitive Strategies in The Lodging Service Sector : Five Porter Analyses And Case Study SWOT Analysis," *J. Bus. Manag. Rev.*, vol. 3, no. 1, pp. 001–017, 2022, doi: 10.47153/jbmr31.2732022.