Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 44 Issue: 06-2025

NATIONAL DEFENSE STRATEGY IN FACING INFORMATION WARFARE IN THE DIGITAL ERA

Winarto[1], Retno Saraswati[2], Lazarus Tri Setyawanta[3]
[1]Doctoral Law Program, Faculty of Law, Diponogoro University, Semarang
[2,3]Lecturer in Law, Faculty of Law, Diponegoro University, Semarang
Jl. Prof. Soedarto, SH., Tembalang, Semarang
winarto@students.undip.ac.id

ABSTRACT

The purpose of this study is to analyze: 1) What are the efforts made by the Indonesian government in protecting state secret information data and resistance to *cyber war*? 2) The country's defense strategy in facing information warfare in the digital era? 3) How are efforts to reconstruct the formation of a national *cyber defense* or *cyber army* in an effort to defend state sovereignty?. This research is a type of normative juridical research with a legislative approach, a conceptual approach, and a case study.

The results of the study show that: 1) Related to efforts to ensure legal certainty in the development of *cyber-security* has been carried out, among others, by implementing a series of programs that have begun to run, including: initiating laws and regulations related to *cyber-security* such as the Electronic Information and Transaction Law No. 11 of 2008, Government Regulation on the Implementation of Electronic Systems and Transactions No. 82 of 2012, which compiles a national framework *for cyber-security*. 2) In order to overcome cyber crime, the policy that has been implemented by the Ministry of Defense and Security is to form a Cyber *Defence Operation Center Working Team* which aims to maintain internal security and protection (Kemhan) as well as external security and protection (national) in the cyber world. *The Cyber Defence Operation Center* in the level of national cyber-security policy is aimed at building a universal defense system that involves all citizens, regions and other national resources to uphold state sovereignty, territorial integrity and the safety of the entire nation from the threat of cybe. 3) The Ministry of Defense is an agency that has full authority in the formation of cyber armies. Various ways can be done in recruiting cyber soldiers such as TNI recruitment in general, or recording all current TNI members who have more abilities and expertise in the IT field to be transferred to become cyber soldiers who will of course be given special training on cyber and *cyber force*.

Keywords: Strategy, Defense, State, War, Information, Digital Age

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 44 Issue: 06-2025

INTRODUCTION

Background

IT provides benefits, as well as being a threat to the country. IT threats to the state can be used to carry out *cyber attacks*, for example as spying, network exploitation, theft of confidential information from companies or the state, and other activities. Cyber *attack* activities can be carried out through cross-border attacks that can be carried out by the international community or countries. *Cyber attacks* on *cyberspace* networks are a threat to global network security. The threat of cyber attacks not only attacks developing countries or countries that are weak in technology, but can also attack developed countries that have more modern IT networks.[1]

In this case, the need to strengthen the State defense system is a priority agenda. Problems and strategic issues that are priorities in the field of defense and security. The realization of a sovereign, independent and personality Indonesia based on mutual cooperation, with a special mission in the field of defense and security is to realize national security that is able to maintain territorial sovereignty, support economic independence by securing maritime resources, and reflect Indonesia's personality as an archipelagic country.[2]

Reviewing the current realities both domestic, regional, and global that affect national interests directly or indirectly. Domestically, Indonesia's strategic environment is characterized by socio-political stability and sustainable economic growth, while at the regional and international levels there is competition as a result of the redistribution of world power concentrated in the Asia Pacific.[3]

Law Number 3 of 2002 concerning State Defense states that State Defense is all efforts to defend state sovereignty, the territorial integrity of the Unitary State of the Republic of Indonesia, and the safety of the entire nation from threats and disturbances to the integrity

[1] Syafrinal Syafrinal and Abdus Salam, "Network Security to Protect Negative Web: A Case Study of the Government of Aceh," *Jurnal Mantik* 5, no. 3 (2021): 1584–90.
[2] Muhammad Prima Ersya, "Legal Problems in Overcoming Cyber Crime in Indonesia," *Journal of Moral and Civic Education* 1, no. 1 (2017): 50–62.
[3] Maskun Maskun et al., "The Legal Position of Cyber Crime in the Development of Contemporary International Law," *Legal Issues* 42, no. 4 (2013): 511–19.

of the nation and state. All matters related to the implementation of integrated defense activities are held in a state defense system.[4]

In essence, state defense is all universal defense efforts whose implementation is based on awareness of the rights and obligations of citizens and belief in one's own strength, which aims to maintain and protect state sovereignty, the territorial integrity of the Unitary State of the Republic of Indonesia, and the safety of the entire nation from all forms of threats. Therefore, Indonesia's defense system must be placed as one of the country's fundamental systems to be able to answer all threats and security challenges that the nation will face in the future.[5]

Meanwhile, in dealing with non-military threats, government institutions outside the defense sector are placed as the main element, in accordance with the form and nature of the threats faced with the support of other elements of the nation's strength. State defense is organized through efforts to build and foster the capabilities and deterrence of the state and nation, as well as overcoming every threat. State defense is organized by the government and prepared early with the state defense system.[6]

The occurrence of cyber war in Indonesia is related to political and social problems that occur, for example when there is a racial riot, Indonesia fights in cyberspace with hackers from various countries. In recent years, there has also been a cyber war between Indonesia and Malaysia. The mutual involvement between hackers from the two countries colored this feud. This action usually occurs when there is a political conflict or competition between the two countries. Although it did not involve the governments of the two countries, the actions of these hackers attacked cyber facilities owned by the Malaysian and Indonesian governments.[7]

Some countries already have special units of cyber forces in their national defense and security. The agency or organization is in charge of gathering all defense efforts and counterattacks on security in the cyber world and its network systems. Seeing the strengths

[4] Law Number 3 of 2002 concerning State Defense
[5] Bagus Artiadi Soewardi, "The Need to Build a Resilient Cyber Defense System for Indonesia," *Defense Potential*, 2013, 31–35.
[6] Defense, "Indonesian Defense White Paper."
[7] Koloay, "The Development of Indonesian Law Regarding Information and Communication Technology By: Renny Ns Koloay."

and threats that can occur due to advances in information technology, many countries are starting to build the strength of their cyber war forces. Because this war is no longer just a virtual game and a fictional story, but has become part of the world stage. Efforts made by the Indonesian government in protecting state secret information data and resistance to *cyber war*, and efforts to reconstruct the formation of a national *cyber defense* or *cyber army* in an effort to defend state sovereignty[8]

This is intended so that the implementation of state defense is in accordance with international legal rules related to the principle of differentiating the treatment of combatants and non-combatants, as well as for simplifying the organization of state defense efforts. In addition, this Law also regulates natural resources, artificial resources, and national facilities and infrastructure, both as reserve components and supporting components.[9]On the basis of these problems, this study will examine and analyze more deeply ***the "State Defense Strategy in Facing Information Warfare in the Digital Age"***

Problem Formulation

1. What are the efforts made by the Indonesian government in protecting state secret information data and fighting cyber *war*?
2. The country's defense strategy in facing information warfare in the digital era?
3. How are efforts to reconstruct the formation of a national *cyber defense* or *cyber army* in an effort to defend state sovereignty?

THEORETICAL FRAMEWORK

1. *Grand Theory* of Law Enforcement and Authority

Authority is not only interpreted as the right to exercise power. However, authority is also interpreted, namely: To implement and enforce the law; Definite obedience; Command; Decide; Supervision; Jurisdiction; or power. In general, authority is defined

[8] I Gusti Agung Ayu Dike Widhiyaastuti, "The Phenomenon of Cyber Terrorism," *KERTHA PATRIKA*, n.d., 78.
[9] Darmawan Napitupulu, "A Study of the Role of Cyber Law in Strengthening the Security of the National Information System," *Deviance Journal of Criminology* 1, no. 1 (2017): 100–113.

as power, power is "the ability of a person or group to control another person or group based on authority, charismatic authority or physical strength"

Hassan Shadhily clarified the translation of authority by giving a definition of "delegation *of authority*". *Delegation of authority* is the process of handing over authority from a leader (manager) to his subordinates (*subordinates*) accompanied by the responsibility to perform certain tasks. The delegation of authority process is carried out through the following steps: determining the duties of the subordinates; the delegation of authority itself; and the obligation to perform the tasks that have been determined.

From the various definitions of authority as mentioned above, it can be concluded that authority or authority has a different meaning from authority or *competence*. Authority is a formal power that comes from the law, while authority itself is a specification of authority which means that whoever here is a legal subject who is given authority by law, then the legal subject is authorized to do something within the authority because of the order of the law.

2. *Middle Theory Cyber War*

There are several definitions that explain the concept of cyber war. Cyber war is a war that uses computer networks and the internet or cyberspace in the form of defense strategies or attacks in the enemy's information system. The Congressional Research Service Report notes that cyber warfare can be used to describe various aspects of defending and attacking information and computer networks in cyberspace, as well as being able to deter adversaries from doing the same.[10]

According to the United Nations (UN) *Security Council Resolution, cyber warfare* is the use of computers or digital means by governments or with explicit knowledge or consent from governments in other countries, or private property in other countries including: intentional access, data capture or damage to digital technologies and

[10] Widhiyaastuti, "The Phenomenon of Cyber Terrorism."

control of digital infrastructure. *Cyber warfare* refers to the use and network of computers to wage war in *cyberspace*.[11]

Cyber warfare can cripple a country's network and access to network control, by using malware such as viruses and worms as cyber weapons to attack and damage digital network systems. Cyber war can be involved in espionage, criminal activities, and economic warfare. The measures are designed to support military operations at the tactical and operational levels of war, as well as independent operations used to achieve strategic effect. The main focus of independent cyber war operations is to achieve strategic effects (i.e. to inflict damage in the country that is affected by the cyber attack).[12]

3. Aplied Theory Network Security

Network security or also known as cyber security is the protection of computers, electronic information and/or digital networks against unauthorized notifications, transfers, rejections, intentional or accidental modification or destruction. The convenience brought by IT provides advantages for the public in accessing the global information network. IT is experiencing rapid development, unwittingly and bringing changes in the international community.[13]

Global information networks can bring various types of cyber threats. The threat of cyber attacks brought by the flow of internet network traffic can be a threat to a country's cyber security. Moreover, today nations have attachments and dependencies on global IT networks in carrying out various activities.[14]

[11] Widhiyaastuti.
[12] Situmeang, "Cyber Law."
[13] Napitupulu, "A Study of the Role of Cyber Law in Strengthening the Security of the National Information System."
[14] Nadia Talita Putri, Idin Fasisaka, and A A B Surya Widya Nugraha, "HANDLING CYBER ATTACKS BY THE CHINESE GOVERNMENT THROUGH NETWORK SECURITY POLICY IN 2000-2015," n.d.

RESEARCH METHODOLOGY

The research in this article is included in the type of doctrinal research, where the approach method used is normative juridical. The discussion of problems related to the country's defense strategy in facing information warfare in the digital era is carried out by prioritizing secondary data derived from the results of literature studies and documentation studies of national and international laws and regulations.[15]

In this study, the way to access and research is mostly taken from literature materials, namely materials that contain new or cutting-edge scientific knowledge, or new understandings of known facts or ideas or ideas. In this case, it includes books, journals, dissertations or theses and other legal materials. This normative law research fully uses primary legal materials and secondary legal materials.[16]

RESEARCH RESULTS

Efforts made by the Indonesian government in protecting state secret information data and resistance to *cyber war*

Cyber crime and Cyber War are not only threats that attack individuals but also threats to business and industry fields as well as vital objects of government. The creation of public and international opinion on an intention such as for campaigns to propaganda. With information technology and the internet, these actors can do it in an easy way, using more efficient costs and resources. Cyber attacks are espionage efforts on industries and vital government objects such as hostage-taking and destruction of important confidential information can cause anxiety and insecurity due to the loss of personal boundaries and the threat of loss of assets and wealth. Not only that, if this cyber attack attempt occurs, it can be used for political purposes, cyber can also be used as a political tool such as spreading hoax news with the aim of political provocation to engineering the economic sector. Internet

[15] S H I Nor Salam, *INTERDISCIPLINARY ISLAMIC LAW RESEARCH METHODOLOGY Elaborate on the Philosophy of Science and Islamic Sciences* (CV Literacy Nusantara Abadi, 2021).
[16] Zainal Asikin, "Introduction to Legal Research Methods," 2016.

interconnection also allows attacks aimed at disabling and destroying the resources of the opposing country without the need to approach the object.[17]

Currently, *cyber attacks* are the latest method to compete and even direct attacks on a country's defense. This attack refers to the use of deliberate activities to disrupt, alter, degrade, deceive, or damage network/computer systems used by adversaries or population information and/or programs. The problem arises when cyberattacks are considered to provide military benefits and are aligned with disputes over the use of weapons. These problems cause *latent tensions*, then each country makes efforts to collect various kinds of information about the opponent (*Cyber Recon*). The next stage, *Initiating Event*, is to prepare various kinds of equipment, troops, methods and build strategies, techniques and tactics in carrying out attacks. Next, carry out cyber mobilization (*Cyber Mobilization*) and the last stage is how to start an attack by conducting a cyber attack or *cyber attack* on cyber infrastructure (hospitals, aviation infrastructure, energy infrastructure, etc.) in the context of *cyber war*. These five stages are called *the Cyber Early Warning Model.*

The development of cyber threats has increased rapidly with any actor, both state and non-state. On the other hand, Indonesia is included in the category of very vulnerable countries and is the most potential target in Asia. Very severe cyber threat intrusions have already occurred, such as data theft and destructive misuse of government and private information systems. Cyber threats are an alternative because of their advantages that do not require large costs, minimal use of personnel, anonymity, and can be controlled from different locations to across countries and continents.

The existence of cyber attacks is increasingly evident as evidenced by the state's active involvement in cyber attacks. In response to this, Indonesia must be active in mapping every potential cyber attack in order to maintain national security and resilience, considering that the effects of cyber warfare are very clear and in direct contact with people's lives. Cyber

[17] Tamarell Vimy, et al, The Threat of Cyber Attacks on Indonesia's National Security, Journal of Citizenship Vol. 6 No. 1 June 2022, 2323.

attacks can damage consumer data, turn off electricity and water lines in a city, cause chaos, and even spark the emergence of things that disrupt national stability.[18]

Currently, Indonesia's cybersecurity situation is at a very critical and dangerous stage. This is due to the increase in global information in Indonesia's national information network system. Indonesia is now a prime target for hackers and has overtaken China, making it even more difficult to control the flow of information. This situation can trigger cybercrime globally, which if not properly controlled can paralyze national information systems. Therefore, important attention must be paid to this situation. Legal certainty in cybersecurity policy is needed to prevent the weakening of defense and cyber security in Indonesia.[19]

In 2007, the Minister of Communication and Information Technology issued Decree No. 26/PER/M.Kominfo/5/2007 concerning Securing the Use of Internet Protocol-Based Communication Networks, which was later amended by the Decree of the Minister of Communication and Informatics. Information Technology NO. 16/PER/M.KOMINFO/10/2010. The regulation was updated with the Decree of the Minister of Communication and Information Technology No. 29/PER/M.KOMINFO/12/2010. This rule is used as the basis for ID-SIRTII. ID-SIRTII. Defined by: Monitoring, early detection, early warning of internet network threats. This regulation is used as the basis of IDSIRTII. ID-SIRTII. Assigned to:

1. Coordinate with domestic and foreign parties to improve network security on the internet.
2. Operating and developing the ID-SIRTII database system.
3. Compile a catalog of network utilization.
4. Providing services for telecommunication threats and security based on internet protocols.
5. Become a contact point with institutions in the use of telecommunication networks.
6. Develop an internet-based telecommunication network security work program.

[18] M. Yusuf Samad1 & Pratama Dahlian Persadha, Understanding Russian Cyber Warfare and the Role of State Intelligence Agencies in Countering Cyber Threats, Journal of Science and Technology-KOM (Journal of Science and Communication Technology) Vol. 24 No. 2, December 2022, 135 - 146

[19] Mohammad Makbu et al, Indonesia's Cyber Defend Policy in the Context of Handling International Cyber Threats, YUSTITIA Journal Vol. 23 No. 2, December 2022

7. Develop an internet-based telecommunication network security work program.

Related to efforts to ensure legal certainty in the development of *cyber-security*, among others, by implementing a series of programs that have begun to run, including: initiating laws and regulations related to *cyber-security* such as the Information and Electronic Transactions Law No. 11 of 2008, Government Regulation on the Implementation of Electronic Systems and Transactions No. 82 of 2012, compiling a national framework *cyber-security*.[20]

Limitations of Overseas Server Services and need to use a secure system; There is no legality that is sufficient to handle cyber attacks; The administration of Cyber Security Institutions is still partial and scattered and there is no coordination standard in dealing with cyber security issues. Cyber Security Processing must be strongly integrated and the involvement of various parties, such as: Intelligence, Law Enforcement, Defense and good security is the defense service and the TNI and the government as regulators, represented in this case Kominfo and the National Crypto Agency which has now been transformed into the State Cyber and Cryptography Agency (BSSN). In order to fight cybercrime, of course, Indonesia is complicated. In order to respond to the increasingly complex cybercrime, it is natural for Indonesia to place the cyber dimension in the context of "national defense and security" by presenting: (1) the construction of its structural base such as the creation of a Cyber Force complementing the Army, Navy, and Air Force; (2) the construction of infrastructure bases such as the strengthening of special satellites for defense and cybersecurity, including this; (3) monitoring the Cyber traffic work protocol which is legally included in the territory of Indonesia, but is technically controlled by a number of telecommunication providers who own the power of the technology where the equipment is purchased, foreign technology.[21]

Regarding *cyber-security* policies in Indonesia, it is necessary to regulate a policy that regulates various elements related to *cyber-security* in various policies that regulate the

[20] Handrini Ardiyanti, Cyber-Security and Its Development Challenges in Indonesia, Politica Vol. 5 No. 1 June 2014
[21] Andrea Angeline et al, TNI Professionalism in the Era of Indonesian Cyber Security and Defense, Das Sollen: Journal of Contemporary Legal and Social Studies (2023) 1:2, 1-25

information and communication technology systems used which include the need for standard documents that are used as a reference in carrying out all processes related to information security, infrastructure standards that must be met in accordance with International standards in dealing with cyber war include the existence of an adequate *perimeter defense*, the existence of *a network monitoring system*, *system information and event management* that functions to monitor various events on the network related to security incidents, network *security assessment* which plays a role in security control and measurement.[22]

The Country's Defense Strategy in Facing Information Warfare in the Digital Era

In the era of globalization where the interconnectedness and dependence between nations and between people around the world through trade, investment, travel, popular culture, and other forms of interaction makes the boundaries of a country become narrower. Everyone in the world can connect with each other, people in the world can talk to each other, chat, connect with each other because of technological advances. Ohmae (1990) stated this as the bordeless world or known as the world without limits. This allows the limited real world because different countries are separate, can become one place, one world because of the influence of technology and globalization, which will certainly make dangerous ideologies, foreign cultures that are not Indonesian culture, misleading teachings, and various threats to the nation's ideology so that the unity and unity of Indonesia can be at stake.

From the defense aspect, cyberspace has become the fifth domain that can be used as a battlefield, in addition to the battlefield of land, sea, air and space, because the use of internet-based systems, equipment, and platforms tends to be increasingly widespread which has the potential to become a vulnerability. The United Nations (United Nations) has also issued decision Number 55/63, which contains that it has been agreed that all countries must work together to anticipate and combat crimes that abuse information technology. An important point in this decision is that every country must have a law or legal regulation capable of eliminating cybercrime. The development of this world is very fast and dynamic,

[22] Handrini Ardiyanti, Cyber-Security and Its Development Challenges in Indonesia, Politica Vol. 5 No. 1 June 2014

state defense readiness and strategy are needed to anticipate it so that security can be created in the face of threats in the life of the nation and state.[23]

Crimes against state security are exclusively enshrined in the Criminal Code (Criminal Code) in the Second Book of Chapter I concerning Crimes Against State Security. The crime of espionage is classified as a crime that has the potential to threaten the stability of Indonesia's defense and security. The article only discusses direct espionage actions carried out by penetrating into defense areas prohibited by the Indonesian Government. It is still unclear if the perpetrator is not an army or armed forces of a country that is in wartime, but personally but at the provocation of the government of a foreign country. Considering that the object is a country that is comprehensively related to the issue of stability, defense and security of the country. Because basically political intersection will participate in influencing espionage acts. Furthermore, the weakness of this Article is that the form of spying is still very classic where virtual conditions have often been used in carrying out criminal acts so that if the espionage case is carried out without physical contact, it will very easily escape the snares of the Article.[24]

Efforts to increase the world's commitment to cybersecurity have been carried out by the Global Cybersecurity *Index (GCI*) ranking by the International Telecommunication *Union (ITU*) of its 193 member countries. The rating is given on the basis of 5 pillars, namely: 1) legal/legal, 2) technical and procedural, 3) organizational structure, 4) capacity building, and 5) international cooperation. Based on the GCI assessment in 2020, Indonesia is ranked 77 out of 193 members. What should be worried about the GCI report is the fact that the development of cybersecurity policy in Indonesia is at 0% when considering how many cyber attacks Indonesia has suffered over the past 5 years.

The government's challenges in the current society 5.0 era in strengthening cyber security include: insufficient availability of technology experts and security technical experts to design and implement *cyber security strategies.* The risks that occur due to the cross-border *nature of cyber security*, which makes countries with weak cyber security resilience

[23] Tamarell Vimy, et al, The Threat of Cyber Attacks on Indonesia's National Security, Journal of Citizenship Vol. 6 No. 1 June 2022, 2323.
[24] Evi Dwi Hastri, *Cyber Espionage* as a Threat to Indonesia's National Defense and Security, LAW AND JUSTICE REVIEW JOURNAL, 2021, Vol. 1, No. 1, 12 – 25

strategies can interfere with the cybersecurity of other countries. The use of anonymization tools, for example to block chain currencies or encryption, in crimes using the internet, further complicates policymaking.[25]

The constant emergence of new technologies and systems from time to time requires periodic updates to the surveillance system. The existence of a new type of communication service provider that is often domiciled in the jurisdiction of another country and requires different treatment compared to traditional telecommunications companies. New forms of *cyber crime* such as*ansomware*, identity theft, sexual approach (*grooming) and* sexual harassment through the cyber realm. The need to deal with cyber attacks and other forms of conflict between countries due to the absence of internationally applicable norms and regulations that govern state behavior. Meanwhile, the challenge for the private sector and businesses is the difficulty of operating across jurisdictions, which means being faced with different laws, penalties and regulatory regimes. Potential to be subject to serious defamation and civil lawsuits if involved in or responsible for a *cyber security* incident. Pressure to assist governments in enforcing *cyber security* as well as countering *cybercrime* and terrorism, which can include policymaking and content reporting, shutting down networks, blocking services, and even compromising the security of their own products to aid government oversight. It is imperative to build internal capacity to maintain information and network security. And in the form of incentives to maintain data confidentiality that can pose risks and cyberattacks in the name of data privacy and potential defamation.[26]

In order to overcome cyber crime, the policy that has been implemented by the Ministry of Defense and Security is to form a Cyber Defence Operation Center Working Team which aims to maintain internal security and protection (Kemhan) as well as external security and protection (national) in the cyber world. The Cyber Defence Operation Center in the level of national cyber-security policy is aimed at building a universal defense system that involves all

[25] Januri et al, Police Efforts in Countering Organized Cyber Crime, Audi et AP : Journal of Legal Research, 01 (02), 2022: 94-100
[26] Eko Budi et al, Strategies for Strengthening Cyber Security to Realize National Security in the Era of Society 5.0, Proceedings of the Indonesian National Seminar on Science, Technology and Innovation Volume 3, Year 2021, pp. 223-234

citizens, regions and other national resources to uphold state sovereignty, territorial integrity and the safety of the entire nation from cyber threats.[27]

The training program and improvement *of cyber security* skills is carried out in coordination with the Cyber *Defence Operation Centre Working Team*. In addition, it is necessary to develop human resources about the importance of *cyber security* to increase understanding of preventive measures in warding off all *cyber crimes*. Rearranging the defense system based on *cyber defence* and *cyber security*, which of course requires careful and systematic preparation with the support of various parties. Synergy in dealing with *cyber* threats is a necessity and a must for Indonesia. With synergy and communication, coordination, networking, and technical cooperation must be carried out to form a cyber security community that can counteract, detect, fend off, and prevent early various potential cyber threat attacks so that it can strengthen national security and resilience.[28]

From an institutional aspect, Indonesia actually has several institutions responsible for cybersecurity, such as the Directorate of *Cyber Crime* at the National Police Headquarters Investigation and Crime Agency (Bareskrim) which is responsible for cybercrime investigations. In addition, on May 4, 2007, Ministerial Regulation No. 26/PER/M. KOMINFO/5/2007 concerning the Security of the Utilization of Internet Protocol-Based Telecommunication Networks was issued. The Minister of Communication and Information Technology in this case appointed the Indonesia *Security Incident Response Team on Internet and Infrastructure/Coordination Center* (ID-SIRTII/CC) which is tasked with supervising the security of telecommunication networks based on internet protocols, the Government has also established the State Cyber and Cryptography Agency (BSSN) in accordance with Presidential Regulation Number 53 of 2017 signed by President Joko Widodo on May 19, 2017. BSSN is a non-ministerial government institution that is under and responsible to the President, the establishment of BSSN is a strengthening of the State Cryptography Institute

[27] Handrini Ardiyanti, Cyber-Security and Its Development Challenges in Indonesia, Politica Vol. 5 No. 1 June 2014
[28] Eko Budi et al, Strategies for Strengthening Cyber Security to Realize National Security in the Era of Society 5.0, Proceedings of the Indonesian National Seminar on Science, Technology and Innovation Volume 3, Year 2021, pp. 223-234

which is supplemented by the Directorate of Information Security. In the Presidential Regulation, it is stated that BSSN is tasked with implementing cybersecurity effectively and efficiently by utilizing, developing and consolidating all elements related to cybersecurity.[29]

It is hoped that the presence of these institutions will present strong cyber security standards in the country, with increasingly rigid duties and authorities in securing the cyber area so that it can ward off any threat of cybercrime that can harm both individuals and institutions and corporations, Indonesia as a country with the fourth most populous population in the world followed by the largest internet penetration in the world, vigilance must be maintained, and should not only be a country that is positioned as a buyer and user but can be an important player, especially in the Southeast Asian region in cyber affairs, must have a strong defense, with the mastery of cyber technology and defense against cyber attacks, it is expected to support and strengthen National Resilience.[30]

BSSN has a national policy direction and strategy to overcome strategic issues in maintaining national security stability in cyberspace, namely strengthening cyber security and resilience which is manifested by the following strategies: a. Strengthening cyber infrastructure security. b. Development and strengthening of the Computer Emergency Response Team (CERT). c. Prevention of cybercrime and increasing international cooperation in the cyber field. d. Strengthening the capacity of cyber security human resources. e. Settlement of cybercrime clearance rate for cyber crimes. The above strategy is the implementation of the five pillars of GCI 2017 which will be implemented for 2020-2024. In this case, Indonesia is in the stage of standardizing the formation of the National Cyber Security so that to achieve ideal cyber security still requires a process in the future. Through

[29] Ahmad Candra et al, INDONESIA FACING THE THREAT OF CYBER WARFARE: A STRATEGY ANALYSIS, rnal Defense Vol 7. No. 3 (2021) pp. 441-451
[30] Sugeng Santoso, Strengthening Cyber Defense to Increase National Resilience, Journal of Lemhannas RI Studies, Edition 34, June 2018, 47.

this strategy, it is hoped that BSSN as a leading sector will be able to optimize its role to realize ideal cyber security for Indonesia.[31]

Efforts to reconstruct the formation of the National *Cyber Defense* or *Cyber Army* in an effort to maintain state sovereignty

The desire for the birth of a Cyber Force that can complement the Army, Navy, and Air Force must be addressed properly and correctly. This is a challenge for the Indonesian government to be biased in presenting a reliable and quality cyber defense and security system for its people. Apart from structural challenges, another challenge in developing Cyber Security policies in the future is the nature of cyber threats that are "*geometric and infinite*" , making their handling not only the responsibility of the TNI, the National Police, the Ministry of Defense, and the Ministry of Communication and Information. One of the interesting strategies that should be considered to deal with global cyber threats includes the government's serious efforts to handle cyber security nationally supported by the private sector and the public for cyber to protect telecommunications and cyber infrastructure from critical situations.

This Cyber Force will be part of the structural formation in the Indonesian National Army (TNI) by developing a national strategy in building Cyber Security in Indonesia in the future. In addition, the Cyber Force is divided to solve problems and support the development of Indonesia's information technology which is not only in the military realm, but also reaches the civilian realm in building national and global Cyber Security that can help the country. The tasks carried out by the Cyber Force are expected to be the center of control over the national information system, information organization competition, information organization decision-making, and information system functionalism in two domains in question by collaborating with other cyber institutions.[32]

[31] Yusep Ginanjar, Indonesia's Strategy to Shape Cyber Security in Facing the Threat of Cyber Crime through the State Cyber and Cryptography Agency, Journal of Global Dynamics Vol.7 No. 2, December 2022
[32] Andrea Angeline et al, TNI Professionalism in the Era of Indonesian Cyber Security and Defense, Das Sollen: Journal of Contemporary Legal and Social Studies (2023) 1:2, 1-25

Hidayat Chusnul Chotimah (2019) said that in dealing with cyber threats, the most important thing is good cyber threat handling management by the State Cyber and Cryptography Agency, in other words this institution must really be able to function or function to anticipate cyber threats, as well as maintain national cyber security and sovereignty. Nur Khalimatus Sa'diyah and Ria Tri Vinata (2016) in research related to the reconstruction of the formation of national *cyber defense* described the solutions or ways to deal with hybrid warfare (cyber warfare) nationally, namely; **First;** creating/perfecting special TNI doctrine related to the concept of facing the threat of hybrid war, it is also necessary to improve the legal and legal dimensions as well as policies in relation to *cyber security*, including the need to establish cyber warfare units such as the National *Cyber Defense/Cyber Army* or *Cyber Warrior* which has the ability to conduct electronic warfare, especially *cyber defense* and *cyber attack*. *Second*; Increasing human resources through domestic and foreign training to achieve human resources who have the ability to carry out hybrid warfare which include software experts, anti-haecker experts, information experts, telematics experts, explosives experts, atomic physicists, biologists, and military tactics experts. *Third*; The development of joint satellites in carrying out cyber warfare missions includes NCW information system technology satellites/*Centric Warfare networks*, SIPRNet infrastructure, and spy satellites, including GPS satellites. These three satellites are then detailed on 4 needs in hybrid warfare including, first; satellites to study space. Second; telecommunications satellites, third; military satellites equipped with laser weapons and fourth; sky monitoring or astronomical satellites.[33]

Another challenge in the future in the development of cyber-security policies is the nature of cyber threats that are multidimensional, making handling them not only the responsibility of the TNI and/or the National Police. Ministry of Defense and Ministry of Communication and Information. According to Sjafrie Sjamsoeddin, cyber threats are included in asymmetric threats whose handling requires a comprehensive approach. Because of its multidimensional nature, making *cyber-security* is not and is not the business of only one

[33] Salomon A.M. Babys, The Threat of Cyber Warfare in the Digital Era and Indonesia's National Security Solutions, JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021, 436

ministry, but also the business of various other ministries. Therefore, a *cyber-security* policy or *Cyber defence* is needed, the implementation of which requires a coordinating body.

Related to the organization of *cyber-security countermeasures.* One of the interesting strategies that should be observed in dealing with cyber war includes the serious efforts of the United States government in developing The National *Cyber Security Division* (NCSD) or a special division tasked with handling cyber security nationally which is supported by the private sector and the public who have the task of building and maintaining an effective national cyber security system or cyberspace. create and implement a risk management program for the cyber world to protect telecommunications and cyber infrastructure from critical situations known as *the National Cyber Space Response System*. The establishment of a special command for cyber units by the Ministry of Defense led by General Keith Alexander in 2009 is a strategic step that needs to be implemented immediately in an effort to respond more seriously in the framework of defense and maintain sovereignty in the cyber field.

The seriousness of the U.S. military shows that cyber in the framework of defense, is seen not only as a network but has been positioned as a battlefield that must be won. This view makes the US military seriously improve its country's defense system in the cyber field with the command of the military, civilians and stakeholders who have capabilities in the field of information technology as a supporting system to build defense system strategies and tactics that are constantly updated in accordance with rapid developments in cyber and expand the boundaries of existing defense strategies. The struggle to dominate the cyber world in the view of *the US Army Cyber Command* is an integral part of cyber warfare or cyber war itself both now and in the future.

Various threats in the cyber world or cyber threats demand a new approach to managing information, securing information and that is the challenge and condition that drives the formation of *the US Army Cyber Command*. *Cyberspace* or the cyber world itself is placed by the United States on par with other dimensional domains, namely land, sea, air and space. The *U.S. Army Cyber Command* is therefore tasked with planning, coordinating, integrating, synchronizing, and conducting activities to: direct Defense and Defense Department-

designated operations and information networks; prepare for, and when directed, conduct the full spectrum of cyber military operations to enable action in all domains, ensure American security in the cyber world and counteract the various threats that exist in the cyber world.

With the existence of a special command of cyber units, the management of cyber risk management through efforts such as increasing training, information on security and confidentiality as well as building a safe and resilient network to form a resilient cyber defense industry, among others, by creating cyber defense and protection programs that can be used to protect various public and government service systems as well as the military from cyber attacks. only in the form of the Cyber *Defence Operation Center Work Team* as formed by the Ministry of Defense.

The organization related to *cyber security* should be in line with the organization of the use of information technology systems by paying attention to four main things, namely: *first,* information systems and organizational *competitions*; **third**, *information systems* and *organizational decision making*; **Fourth,** organizational *use of information systems*.[34]

Another country known to have a special cyber force unit is Israel. A special unit from Israel was named Unit 8200 with cyber warfare specialists. This unit stands under the auspices of *the Israel Defense Forces* (IDF) which has successfully stopped the radar operation of Syrian anti-aircraft weapons. But the unit was suspected to be the actor of a stuxnet worm attack that attacked the computer systems of Iran's nuclear facilities in early 2011. In addition, Australia is also known to have a special force in cyber security called *the Cyber Security Operations Centre* (CSOC) where this force has responsibility in cyber security, including preventing, detecting, and counteracting all threats and cyber attacks. In addition, China and the UK are also known to have special forces for cyber. The "*Blue Army*" is a special force from China based in Guangzhou, while *the Cyber Security Operations Centre* (CSOC) is a cyber defense system owned by the United Kingdom and based in Cheltenham.

[34] Handrini Ardiyanti, Cyber-Security and Its Development Challenges in Indonesia, Politica Vol. 5 No. 1 June 2014

The number of countries that have been aware of the seriousness of cyber warfare must also be able to encourage the government, especially the Indonesian Ministry of Defense, to immediately form the Cyber Force, as well as the Air Force, Navy, and Army with their overall duties being responsible for national security and defense. Sa'diyah & Vinata (2016) explained that currently the policy regarding force building has been set by the Indonesian Ministry of Defense for the entire TNI. This is certainly good news for Indonesia's defense system which is more prepared for this very rapid change of times. On the other hand, Indonesia's cyber defense certainly still needs more serious handling. Considering that various countries have given serious responses to this cyber war, it is possible that if Indonesia does not have a special unit to handle cyber, Indonesia will be an easy target for cybercriminals in the international arena. In fact, Ardiyanti (2014) explained that Indonesia is the number one country with the highest level of vulnerability in the threat of cybercrime, especially hacking. This is certainly based on the finding that cybercrime in Indonesia has doubled in line with the increase in smartphone and social media users in Indonesia.

The Ministry of Defense is an agency that has full authority in the formation of cyber soldiers. Various ways can be done in recruiting cyber soldiers such as TNI recruitment in general, or recording all current TNI members who have more abilities and expertise in the IT field to be transferred to become cyber soldiers who will of course be given special training on cyber and *cyber force*. Therefore, before the formation of a cyber army, it is necessary to prepare carefully and systematically, such as the availability of detailed and complete budgets, software, hardware, infrastructure, and regulations. Just like other dimensions, *cyber* soldiers must also be evenly deployed in various regions with their command center remaining in the Ministry of Defense. This is intended so that each area can be monitored and protected optimally by *the cyber army.*

Currently, it is known that Indonesia has formed a TNI Cyber Unit which has the main task of protecting the TNI's cyber infrastructure. However, because it is still newly formed, the TNI cyber task force is still in the stage of maintaining cyber security, not yet at the stage of being able to carry out counterattacks. The Ministry of Defense certainly has a long-term plan

to develop cyber defense, one of which is the development of cyber weapons. Of course, this provides good news for the Indonesian defense world considering the various cyber threats that are constantly happening today. Therefore, the development of cyber weapons must also be accompanied by the development of qualified and competent human resources in the cyber field. In the future, the Ministry of Defense is certainly required to further improve the quality of human resources, especially in the cyber sector, in order to create maximum security and defense of the country to face threats both traditional and non-traditional issues.[35]

CONCLUSION

The results of the study show that;

1. Related to efforts to ensure legal certainty in the development of *cyber-security*, among others, by implementing a series of programs that have begun to run, including: initiating laws and regulations related to *cyber-security* such as the Information and Electronic Transactions Law No. 11 of 2008, Government Regulation on the Implementation of Electronic Systems and Transactions No. 82 of 2012, compiling a national framework *cyber-security*.
2. In order to overcome cyber crime, the policy that has been implemented by the Ministry of Defense and Security is to form a Cyber *Defence Operation Center Working Team* which aims to maintain internal security and protection (Kemhan) as well as external security and protection (national) in the cyber world. *The Cyber Defence Operation Center* in the level of national cyber-security policy is aimed at building a universal defense system that involves all citizens, regions and other national resources to uphold state sovereignty, territorial integrity and the safety of the entire nation from cyber threats
3. The Ministry of Defense is an agency that has full authority in the formation of cyber soldiers. Various ways can be done in recruiting cyber soldiers such as TNI recruitment

[35] Krida Eva Setiawan Hasan, The Need for the Indonesian National Army to Have a Cyber Force to Face the Cyber Warfare Era, Journal of Education, Humanities and Social Sciences (JEHSS), Vol 5, No. 1, August 2022: 264-274

in general, or recording all current TNI members who have more abilities and expertise in the IT field to be transferred to become cyber soldiers who will of course be given special training on cyber and *cyber force*.

BIBLIOGRAPHY

Ahmad Candra et al, INDONESIA FACING THE THREAT OF CYBER WARFARE: A STRATEGY ANALYSIS, rnal Defense Vol 7. No. 3 (2021) pp. 441-451

Andrea Angeline et al, TNI Professionalism in the Era of Indonesian Cyber Security and Defense, Das Sollen: Journal of Contemporary Legal and Social Studies (2023) 1:2, 1-25

Bagus Artiadi Soewardi, "The Need to Build a Resilient Cyber Defense System for Indonesia," *Defense Potential*, 2013, 31–35.

Darmawan Napitupulu, "A Study of the Role of Cyber Law in Strengthening the Security of the National Information System," *Deviance Journal of Criminology* 1, no. 1 (2017): 100–113.

Eko Budi et al, Strategies for Strengthening Cyber Security to Realize National Security in the Era of Society 5.0, Proceedings of the Indonesian National Seminar on Science, Technology and Innovation Volume 3, Year 2021, pp. 223-234

Evi Dwi Hastri, *Cyber Espionage* as a Threat to Indonesia's National Defense and Security, LAW AND JUSTICE REVIEW JOURNAL, 2021, Vol. 1, No. 1, 12 – 25

Handrini Ardiyanti, Cyber-Security and Its Development Challenges in Indonesia, Politica Vol. 5 No. 1 June 2014

I Gusti Agung Ayu Dike Widhiyaastuti, "The Phenomenon of Cyber Terrorism," *KERTHA PATRIKA*, n.d., 78.

Januri et al, Police Efforts in Countering Organized Cyber Crime, Audi et AP : Journal of Legal Research, 01 (02), 2022: 94-100

Koloay, "The Development of Indonesian Law Regarding Information and Communication Technology By: Renny Ns Koloay."

Krida Eva Setiawan Hasan, The Need for the Indonesian National Army to Have a Cyber Force to Face the Cyber Warfare Era, Journal of Education, Humanities and Social Sciences (JEHSS), Vol 5, No. 1, August 2022: 264-274

M. Yusuf Samad1 & Pratama Dahlian Persadha, Understanding Russian Cyber Warfare and the Role of State Intelligence Agencies in Countering Cyber Threats, Journal of Science and Technology-KOM (Journal of Science and Communication Technology) Vol. 24 No. 2, December 2022, 135 – 146

Maskun Maskun et al., "The Legal Position of Cyber Crime in the Development of Contemporary International Law," *Legal Issues* 42, no. 4 (2013): 511–19.

Mohammad Makbu et al, Indonesia's Cyber Defend Policy in the Context of Handling International Cyber Threats, YUSTITIA Journal Vol. 23 No. 2, December 2022

Muhammad Prima Ersya, "Legal Problems in Overcoming Cyber Crime in Indonesia," *Journal of Moral and Civic Education* 1, no. 1 (2017): 50–62.

Nadia Talita Putri, Idin Fasisaka, and A A B Surya Widya Nugraha, "HANDLING CYBER ATTACKS BY THE CHINESE GOVERNMENT THROUGH NETWORK SECURITY POLICY IN 2000-2015," n.d.

Napitupulu, "A Study of the Role of Cyber Law in Strengthening the Security of the National Information System."

Defense, "Indonesian Defense White Paper."

S H I Nor Salam, *INTERDISCIPLINARY ISLAMIC LAW RESEARCH METHODOLOGY Elaborate on the Philosophy of Science and Islamic Sciences* (CV Literacy Nusantara Abadi, 2021).

Salomon A.M. Babys, The Threat of Cyber Warfare in the Digital Era and Indonesia's National Security Solutions, JURNAL ORATIO DIRECTA VOL. 3 NO. 1, NOVEMBER 2021

Sugeng Santoso, Strengthening Cyber Defense to Increase National Resilience, Journal of Lemhannas RI Studies, Edition 34, June 2018

Syafrinal Syafrinal and Abdus Salam, "Network Security to Protect Negative Web: A Case Study of the Government of Aceh," *Jurnal Mantik* 5, no. 3 (2021): 1584–90.

Tamarell Vimy, et al, The Threat of Cyber Attacks on Indonesia's National Security, Journal of Citizenship Vol. 6 No. 1 June 2022

Law Number 3 of 2002 concerning State Defense

Widhiyaastuti, "The Phenomenon of Cyber Terrorism."

Yusep Ginanjar, Indonesia's Strategy to Shape Cyber Security in Facing the Threat of Cyber Crime through the State Cyber and Cryptography Agency, Journal of Global Dynamics Vol.7 No. 2, December 2022

Zainal Asikin, "Introduction to Legal Research Methods," 2016.