NATIONAL DEFENSE EFFORTS IN THE FACE OF *ARTIFICIAL INTELLIGENCE THREATS*

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 is the legal basis of artificial intelligence technology? 2) How does AI function in defense systems? 3) What are the country's defense efforts in dealing with AI threats?. 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) The ITE Law as a positive law that applies in Indonesia groups AI into electronic systems and agents where if referring to the characteristics of AI from the definition of electronic systems contained in the ITE Law, there is a lot of harmony because AI has a way of working, one of which is collecting data and then processing it even to the analysis stage and has the ability to convey electronic information in accordance with the what is contained in "Article 1 Number 5 of the ITE Law". 2) The use of AI in defense mostly exists in six main areas, namely; Weapons targeting and autonomous weapons, Surveillance (*intelligence, surveillance, reconnaissance*), Cybersecurity, Homeland security, Logistics, and Autonomous vehicles. 3) To achieve the desired goals in dealing with AI threats in defense and providing support for the security and defense of the State, ways are needed), among others; Establishment of adequate policies, laws and regulations as a basis, Strengthening intelligence capabilities, Development of the domestic defense industry, sustainable recruitment and training of human resources, Integrated force building among the main components, reserves and supporters, and Conducting bilateral, multilateral cooperation at the regional and international levels

Keywords: Effort, Defense, State, Facing, Threats, Artificial Intelligence

INTRODUCTION

Background

Cyber threats are an increasingly important issue in today's digital era. *Cyber threats* are in the form of attacks or illegal actions carried out through networks or information systems, such as the internet. Cyber threats are very diverse and can threaten information security, privacy, and the economy of individuals and organizations. DDoS (*Distributed Denial of Service*) attacks are one example of *cyber threats.* DDoS attacks make a network or website inaccessible by flooding the network with fake traffic. This attack can affect system performance and make customers unable to access the services they need.

The government also plays an important role in cyber defense. Governments can create regulations and laws to ensure that organizations and individuals take adequate measures to protect their networks and information. Governments can also provide technical support and assistance to ensure that cyber defense is effective. Overall, cyber defense is essential for every individual and organization in today's digital age. To ensure that information and networks are secure, there needs to be consistent action and effort from all parties. Security technology, education and awareness, and government support are all critical to ensuring that cyber defenses function properly and protect information and networks from *cyber threats*.

To overcome *cyber* threats, the use of *Artificial Intelligence* (AI) in cyber defense is important. AI has the ability to process and analyze huge amounts of data quickly and accurately. This makes AI very useful in helping to prevent and address *cyber threats*. *Artificial Intelligence* (AI) is a branch of computer science that concentrates on creating machines that can perform roles that humans typically do, such as solving problems, making decisions, and adapting to new situations.[1]

The rapid development of digital technology is increasingly advanced and with various artificial intelligence or *Artificial Intelligence* (AI) in various areas of human life has been widely used. AI has provided significant advancements in several fields such as, industry, healthcare, and public services. However, as it progresses, the threat of cyberattacks can emerge and engage its users. AI cyberattacks are considered detrimental because they attack data security and user privacy. The existence of computer technology has formed a new space which is a

[1] Ishak Farid, et al, The Utilization of Artificial Intelligence in Cyber Defense, NUSANTARA: Journal of Social Sciences, 10 (2) (2023): 779-788

computer-based communication world called *cyberspace*. The new space not only has a good impact but also has a bad impact, often some individuals use it to commit crimes in *cyberspace*, commonly called *cybercrime*. *Cybercrime* is an act of using a computer network that is unlawful by making computers as objects, by profiting from the losses of others.[2]

In Indonesia, there is still a lack of public awareness and understanding of the threat of AI cyber attacks on their data security. Comprehensive research is needed to understand the threats and their impact on data security in Indonesia. The purpose of this study is to provide a better understanding of the threat of AI cyber attacks to data security in Indonesia. With this understanding, it is hoped that effective protection strategies can be developed to counter AI cyberattacks and ensure that user privacy is well maintained. It is hoped that the results of this study will make a significant contribution to raising awareness of the public, government, and private sector in Indonesia about the threat of AI cyberattacks on data security and privacy.[3]

The Rector of the Indonesian Defense University highlighted the important role of big data and Artificial *Intelligence* (AI) in the country's security system. The use of *Artificial Intelligence* (AI) in national defense aims to improve the accuracy of weapon systems, efficient use of resources, and reduce the number of casualties of soldiers in military operations. The use of big data in the field of state defense focuses on validating the process and mechanism of sharing information from various data sources with various types of data. The goal is to compile data in a prioritized manner and enable quick and precise decision-making in the context of military action by building artificial intelligence. Artificial intelligence has revolutionized the world of defense with its incredible capabilities. However, with these advances, challenges also arise that need to be overcome so that the use of artificial intelligence in defense can be implemented effectively. This introduction outlines the importance of understanding these challenges and finding the right solutions.[4]

[2] Marufah, N., Rahmat, H.K. and Widana, I.D.K.K., 2020. Moral Degradation as the Impact of Cybercrime on the Millennial Generation in Indonesia. NUSANTARA: Journal of Social Sciences, 7(1), pp.191-201.

[3] Anastasya Zalsabilla Hermawan, Literature Study: The Threat of Artificial Intelligence (AI) Cyber Attacks on Data Security in Indonesia, Proceedings of the 2023 National Seminar on Information Technology and Systems (SITASI) Surabaya, 6 – 7 September 2023

[4] Ardian Yudopratomo, Challenges to the Future of National Defense Due to Artificial Intelligence, NUSANTARA: Journal of Social Sciences, 10 (8) (2023): 4051-4057

Problem Formulation

1. What is the legal basis of artificial intelligence technology?
2. How does AI function in defense systems?
3. How are the country's defense efforts in dealing with AI threats?

THEORETICAL FRAMEWORK

1. Law Enforcement and Authority Theory

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 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. *Defense theory*

Defense is a concept that has various definitions, especially in the administration of a country. The concept of defense is often associated with aspects of state life with the idea of survival which has a relationship with the sense of security (security) of every resource in the country from all threats that can be sourced from within or outside the country. According to Syarifudin Tippe, the object of defense science is the behavior of the state to maintain and develop the sustainability of the country's life.

Military and war science is the forerunner of defense science which has the essence of concepts and ideas related to the development of military organizations, strategies, and tactics in achieving the interests of the State.[5]

Along the way, various threats that have an impact on the country's defense continue to change as a result of the development of a dynamic environment and strategic context. Military, nonmilitary, and hybrid threats are several different categories of threats that make up the complexity of the threat. These threats can be divided into real and hypothetical threats. .[6]

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.[7]

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.[8]

RESEARCH RESULTS

Legal Basis of Artificial Intelligence Technology

At the beginning of the twentieth century the term technology was used in general terms and encapsulated a set of means, processes and ideas in addition to tools and machines. The expansion of this meaning continued until the middle of this century the formulation of

[5] Tippe, S. (2016). Defense Science: History, Concept and Implementation. Jakarta: Salemba Humanika

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

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

[8] Zainal Asikin, "Introduction to Legal Research Methods," 2016.

technology emerged as "*the means or activity by which means seeks to change or manipulate his environment*".[9]

Law and technology are familiar terms in the era of modernization development like today. The rapid development of the world has been supported by the process of globalization. Of course, the presence of globalization which has a lot of influence on human life in any country brings new opportunities. Initially, the long-distance communication system was difficult to turn into an easy thing with the capital of the internet network and smart devices. This is in line with the digital revolution which aims to facilitate human needs. Since the 1980s, the digital revolution began with a shift in the use of technology that began with a change in the form of mechanical and analog technology to more sophisticated digital technology. Starting from the activity of finding the information needed to online business activities can be done easily through the modern gadgets owned. With this situation, it can be said that the digital era has occurred in today's life and continues to grow rapidly.

Of course, Indonesia has a great opportunity to properly manage the ongoing digital developments. So it is necessary for Indonesia to keep up with existing technological developments, one of which is to be able to create progress in various aspects. Article 28C paragraph (1) of the 1945 Constitution of the Republic of Indonesia states that, "Everyone has the right to develop themselves through the fulfillment of their basic needs, the right to education and benefit from science and technology, art and culture, in order to improve the quality of life and for the welfare of mankind." The mandate for the implementation of Article 28C of the 1945 Constitution of the Republic of Indonesia itself is also in line with the theory put forward by Gustav Radburch, regarding the existence of the law in achieving 3 (three) main goals, namely, Justice; Benefits; and Legal certainty. So in this case, it can be interpreted that the development of digitalization technology in the legal field will certainly bring benefits to all people's lives in providing convenience and/or legal certainty in every procedure for its implementation. Furthermore, related to technological development, it is also supported by the implementation of Article 31 paragraph (5) of the 1945 Constitution of the Republic of Indonesia, which states that in essence the Government must advance science and technology

[9] Ronny Hanitidjo Soemitro, Law and the Development of Science and Technology in Society, Inauguration Speech of Permanent Professor at the Faculty of Law, Diponegoro University, Semarang, December 6, 1990, p.9.

by upholding religious values and national unity for the advancement of civilization and the welfare of mankind.[10]

Indonesia itself is defined as technology, one of which is in Article 1 number 1 of Law of the Republic of Indonesia Number 18 of 2002 concerning the National System for Research, Development and Application of Science and Technology, namely: Technology is a method or method as well as a process or product that results from the application and utilization of various scientific disciplines that produce value for the fulfillment of needs, continuity and improvement of the quality of human life.

The rapid development of technology without being followed by the existence of a legal basis that regulates it will cause confusion in society due to the absence of legal certainty related to it. That it is true that the law lags behind the events that will continue to occur (*Het recht hink achter de feiten aan*), it is just a matter of how the law can keep its distance from the events and developments in this case technology. One of the current technological developments that can be used in the legal field in its efforts to catch up or narrow the lag behind its events is to use or utilize artificial *intelligence* (AI). The reality is that currently AI has been widely used in all areas of life in society, with AI work and human life can be easier and can increase productivity from work results.[11]

The development of the use of technology, especially artificial intelligence in the era of industrial revolution, is increasingly rapid to give rise to a new era or trend, namely the era of artificial intelligence disruption. In general, distrupsin is a process of massive innovation and change that can fundamentally change all existing systems, orders, and landscapes in new ways. This will result in people who still use the old methods and systems will lose competition. Meanwhile, the era *of artificial intelligence* (AI) disruption is an era of innovation and massive change fundamentally due to the presence of artificial intelligence (AI) that can change all systems or orders and landscapes to new ways (which were previously uncommon or never expected).[12]

[10] Farid Abdul, (2019), Digital Phenomena in the Era of the Industrial Revolution 4.0, Journal of DKV Dimension of Fine Arts and Design, 4(1), 48.
[11] Paulus Wisnu Yudoprakoso, Artificial Intelligence as a Tool for the Drafting Process of Laws in an Effort to Face the Industrial Revolution 4.0 in Indonesia, Indonesian Law Symposium Volume 1 Number 1 of 2019, 453
[12] Abdul Hadi, Reform of National Law in Efforts to Protect Personal Data in the Era of Artificial Intelligence Disruption, Mimbar Justitia Law Journal, Vol. 8 No. 1 – June 2022, pp. 233-253.

AI covers a sizable field, from the most general to the niche. From Learning or Perception to chess games, proving mathematical theories, writing poetry, driving a car and diagnosing diseases. The word Intelligence comes from the Latin intellegio which means "I understand", so the basis of Intelligence is the ability to understand and take action.[13]

Some experts give their own definitions related to what AI is, as follows:[14]

a. John Mc Carthy: Artificial intelligence is modeling human thought processes and designing machines to mimic human behavior.
b. H.A. Simon: Artificial intelligence is a place of research, applications and instructions related to computer programming to do something that in the human view is intelligent.
c. Rich and Knight: Artificial intelligence is the study of how computers can do things that humans can do better.

Artificial intelligence or in scientific names called Artificial Intelligence is a computer system that has a special algorithm so that it can act like a human. Artificial intelligence (AI) has the ability to correctly interpret external data, manage data, and use processed results for specific purposes known as artificial intelligence, or intelligence added in computing systems[15]. AI is an interdisciplinary subject that involves thinking, systems, logic, cognition, information, and biology. AI is used in knowledge processing, pattern recognition, machine learning, and natural language processing (NLP). AI has been applied to various areas of life, including automated system programming, expert systems, knowledge systems and smart robots.[16]

Artificial intelligence (AI) is part of the subject of interdisciplinary science involving information, logic, cognition, thinking, systems, and biology. It has been intended for *Knowledge Proccesing, Pattern Recognition, Machine Learning*, and *Natural Language Proccesing* (NLP). The use of AI has been applied to various fields, such as automated programming, expert systems, knowledge systems, and intelligent robots. Not only does AI require logical thinking and imitation, but emotions are also an integral part of it. The next

[13] Widodo Budiharto and Derwin Suhartono, 2014, Artificial Intelligence: Concept and Application, Andi Publishers, Yogyakarta, pp.2-3.
[14] https://pendidikanmu.com/2018/11/pengertian-kecerdasan-buatan-menurut-para-ahli.html
[15] Margaret A Goralski and Tay Keong, "The International Journal of Arti Fi Cial Intelligence and Sustainable Development" 18, no. June 2019 (2020)
[16] Caiming Zhang and Yang Lu, "Study on Artificial Intelligence: The State of the Art and Future Prospects," Journal of Industrial Information Integration 23, no. May (2021): 100224,

breakthrough in the field of AI could not only provide computers with more logical reasoning abilities but could also provide them with emotional abilities. Machine intelligence will soon surpass human intelligence.[17]

AI can increase human capacity by processing and analyzing large data sets much faster than humans. For example, in medical care, AI can help analyze data from a large number of individuals and identify patterns for disease diagnosis. In the legal sector, AI is used to sift through court documents and legal records for information relevant to the case. In the automobile industry, AI-driven robots have been used on assembly lines. Their potential for the defense domain is huge as AI solutions are expected to emerge in critical areas such as cyber defense, decision support systems, risk management, pattern recognition, cyber situational awareness, projection, malware detection, and data correlation.[18]

Regarding the position of legal subjects associated with AI, this certainly raises many debates that have different opinions and perspectives in seeing the position of AI towards the legal acts it does. If the problem of AI as a subject cannot be equated with a legal entity, according to Otto Von Gierke through the theory of organs, the legal entity is actually the real reality of a natural nature and personality of humans in their legal association. Which of course a legal entity has rights and obligations and can act independently in every decision issued as a legal subject. Another opinion of L. J. Van Apeldoorn "to be able to perform a legal act, the subject of the law itself in this case must have the ability to hold the rights given to him" and the meaning of the ability to hold the right is that in terms of capacity it is differentiated like a minor in performing a legal act and a person under custody, in general the person can be given rights that can then be used in carrying out a legal act, However, legally the person is not capable of doing his legal deeds and this determines a legal subject.

AI cannot be equated with a legal entity to be a legal subject, where a legal entity has a clear and firm intention and purpose in its stance and there is a scope of humans, and AI cannot stand independently which as is known, the computer is regulated and programmed by humans and if the computer or AI takes a decision that can be likened to a human then the

[17] Jajang Nurzaman, et al, The Validity of Contracts Made by Artificial Intelligence According to Positive Law in Indonesia, Al' Adl : Jurnal Hukum, Volume 16 Number 1, January 2024, 142

[18] FL. Yudhi Priyo Amboro, & Khusuf Komarhan, The Prospect of Artificial Intelligence as a Subject of Civil Law in Indonesia, Law Review Volume XX, No. 2 – November 2021

perfection in the decision cannot be ensured if not There is human supremacy in decision-making, as computers are not always immune to system errors.[19]

AI is created as well as possible so that it can have human-like intelligence and even exceed humans in carrying out mechanical activities. Jaya and Goh also explained that, in progressive law, the development of AI is one of the breakthroughs that has innovation and novelty. AI can work without being based on humanist feelings or consciousness, so it is able to exceed human ability and speed in solving various mechanical problems. This is the reason, AI can be placed as a legal subject that gets legal certainty according to the positive law that applies in Indonesia. AI has a responsible person, namely the creator and user of AI, each of whom has rights and obligations. Creators and users can create authentic deeds as AI identities. Likewise, government agencies or agencies can also form a special section that handles AI disputes that can occur at any time.[20]

Artificial Intelligence (AI) has a wide legal impact on the entire world community, but the Indonesian legal system itself has not in fact explicitly regulated the existence of *Artificial Intelligence* (AI), especially related to its position of responsibility in the legal industry in Indonesia. The lack of a law regarding decrees related *to Artificial Intelligence* (AI) itself, has resulted in many legal practitioners in Indonesia still taking advantage of regulations related to technology regulation, namely Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions which is then hereinafter referred to as the "ITE Law" this regulation as a form of the state responding to the rapid development of technology in the country. Indonesian.

Therefore, in order to anticipate all possible threats that arise as a result of the lack of regulation related to the existence of Artificial Intelligence (AI), at least some considerations need to be made in the position of Artificial Intelligence (AI) capacity in being responsible. Explicitly, even though Artificial Intelligence (AI) in its position performs all legal actions as if it were a legal subject, AI basically cannot play the role of a legal subject, so it is necessary to interpret the theory contained in legal regulations by providing figurative meaning according to legal principles as a connecting solution in AI regulation.

[19] Muhammad Tan Abdul Rahman Haris & Tantimin, Analysis of Criminal Law Liability for the Utilization of Artificial Intelligence in Indonesia, JOURNAL OF LEGAL COMMUNICATION, VOLUME 8 NUMBER 1 FEBRUARY 2022
[20] Endang Purwaningsih & Irfan Islami, Analysis of Artificial Intelligence (Ai) as an Inventor Based on Patent Law and Islamic Law, Galuh Justisi Scientific Journal, Volume 11 Number 1- March 2023, 9.

Indonesia itself formed the ITE Law with the hope of solving problems related to technology and information systems in order to realize legal certainty and be useful for solving problems related to technology. Unfortunately, AI is not clearly defined in the regulation of the ITE Law where this then leads to a rampant effort to translate AI so that it can be associated with the regulations contained in the ITE Law itself.

The ITE Law as a positive law that applies in Indonesia groups AI into electronic systems and agents where if referring to the characteristics of AI from the definition of electronic systems contained in the ITE Law, there is a lot of harmony because AI has a way of working, one of which is collecting data and then processing it even to the analysis stage and has the ability to convey electronic information in accordance with what is contained in "Article 1 Number 5 of the ITE Law". The grouping of AI into electronic agents basically does not have much difference from including AI in the group of electronic systems on the grounds that AI has the ability to act and perform actions in accordance with the understanding of electronic agents, which are devices that can be controlled by humans as part of an electronic system that can automatically perform actions on electronic systems. This is consistent with the characteristics of AI based on what is contained in "Article 1 Number 8 of the ITE Law".

AI itself basically plays a role as a legal object when referring to legal arrangements that run in Indonesia and cannot be defined as a legal subject. Humans are actors responsible for the operation of AI as a technology, so if it refers to positive law, then humans are the ones who play the role of subjects and this is contained in Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP 71/2019). In other words, the responsibility for the use of AI is fully owned by the organizer from what he or she does when operating the AI with the exception of when there is an emergency that gives rise to the possibility of exemption of such responsibility to the organizer.[21]

The function of artificial intelligence AI in defense systems

The progress of science and technology in a nation is also increasing rapidly in the field of security and defense. One of the greatest dangers to a country's resilience and sovereignty is asymmetric warfare, which can strike at any time and from any location. With advances in

[21] Ni Made Yordha Ayu Astiti, Strict Liability of Artificial Intelligence: Accountability to AI Regulators or Is AI Given the Burden of Accountability?, Udayana Master Law Journal, Vol. 12 No.4 December 2023, 962-980

sensor technology and the capacity of computers to think independently in making shooting decisions, the development of weapon technology has now changed. The defense concept currently in use is based on digital technology, which also has the capacity to hide or keep the forces we have from the opponent and transmit the judgment from the sensors directly to the weapon. In maintaining the secrecy of the war strategy that is currently being planned, strategic information such as intelligence related to enemy forces and the size of our war power must be well stored. It would be even better if we could completely prevent intelligence actions or enemy observation by using sensing technology, namely with drones and satellites. The defense concept that is currently being talked about is Anti Access or Area Denial System, which is conceptually and has been used in traditional wars such as the crusades. The idea of A2 or AD generally refers to defensive tactics that have a priority on prevention or defensive construction that is able to withstand attacks from stronger enemies. Of course, in order to survive or even take countermeasures in order to protect state sovereignty, this defense and attack plan must be able to carry out an integrated integration of each country's defense resources. For example, the existence of the armed conflict in Nagorno-Karabakh, the battle between two former members of the Soviet Union Armenia and Azerbaijan, which took significant casualties, is a very clear illustration of the technological development in the war that has been going on for a while.

When it comes to protecting user assets and the overall online environment, cybersecurity refers to a variety of tools, rules, security ideas, protections, guidelines, risk management techniques, actions, training, and technology. Cybersecurity user organizations and resources include individuals, infrastructure, applications, services, telecommunications systems, connected computer devices, and all information sent and/or stored in a virtual environment. The purpose of cybersecurity is to protect user assets, organizational assets, and organizational assets from security risks that apply in the cyber environment. The purpose of cybersecurity is to protect user assets, organizational assets, and organizational assets from security risks that apply in the cyber environment. Availability, Integrity, which includes authenticity and potential measures to reduce the incidence of rejection, and Confidentiality are common security objectives. Legal Certainty, Technical and Procedural Measures, Organizational Structure, Capacity Building and User Education, and International

Cooperation are the five areas of activity that make up global cybersecurity (including mutual cooperation in efforts to address cyber threats).[22]

Cyber defense is an effort to protect computer systems and networks from cyber threats, such as hacker attacks, malware, and data theft. In the era of increasingly advanced technology, cyber threats are becoming more and more serious and result in great losses for individuals, companies, and countries. To overcome cyber threats, the use of *Artificial Intelligence* (AI) in cyber defense is important. AI has the ability to process and analyze large amounts of data quickly and accurately. This makes AI very useful in helping to prevent and address cyber threats.

Artificial Intelligence can increase human capacity by processing and analyzing large data sets much faster than humans. For example, in healthcare, Artificial Intelligence can help analyze data from individuals and identify patterns for making disease diagnoses. In the legal field, Artificial Intelligence is used as a filter for court documents as well as legal records to obtain information relevant to the case. Their potential for the defense part is huge because Artificial Intelligence solutions are expected to emerge in critical areas such as cyber defense, decision support systems, risk management, pattern recognition, cyber situational awareness, projection, malware detection, and data correlation.

Because there are so many datasets available for analysis, AI is helpful in the field of intelligence. For example, the initial phase of Project Maven involved automating intelligence processing to support anti-ISIL activities. The Project Maven team, in particular, has used computer vision and machine learning algorithms to create an intelligence-gathering cell that will examine video from unmanned aerial vehicles and automatically identify hostile behavior for targeting. In this role, AI is intended to automate a workforce of human analysts who currently spend hours sifting through films to extract useful information, potentially allowing analysts to make more effective and rapid judgments based on data.[23]

Utilization of *Artificial Intelligence* in cyber defense *First*, AI can be used for attack detection. AI can monitor network activity and recognize abnormal patterns. If a pattern is detected, AI can alert network administrators and block attacks before they spread and

[22] Makarim, E. (2018). Indonesian Legal Framework for Cybersecurity. Retrieved from. http://www.nisc.go.jp/security-site/campaign/%20ajsympo/pdf/lecture2.pdf

[23] Corrigan, J. (2017, November 3). Three-Star General Wants AI in Every New Weapon System. Retrieved from. https://www.defenseone.com/technology /2017/11/three-star-general-wantsartificial-intelligence-every-new-weapon-system/142239/

damage the system. AI can be used to assist in detecting attacks on cyber defenses. AI can leverage machine learning algorithms to learn recurring attack patterns and distinguish between normal and unusual activity that may be a sign of an attack. AI can also monitor network activity in real-time and speed up attack detection by processing data at a higher rate than humans.

Second, AI can be used for complementary analysis. AI can learn and analyze normal behavior patterns from users and applications, and alert network administrators if there is a change in those patterns. This helps prevent attacks known as human attacks, such as phishing. In cyber defense, AI can be used to monitor and analyze the activity of networks and information systems to detect potential attacks and threats. AI can also help to predict and prevent attacks by analyzing patterns of abnormal behavior and activity in networks and information systems. Using machine learning algorithms, AI can learn and identify patterns of behavior that can indicate unauthorized attacks or actions, such as searching for confidential data or hacking activity. AI can also help to prioritize cyber defense responses and actions by evaluating threat levels and potential losses. However, it is important to remember that AI also has weaknesses and limitations, such as accuracy issues and errors in pattern recognition, which must be taken into account in the implementation of AI in cyber defense. Therefore, it is important to ensure that AI is used as part of a holistic cyber defense strategy and in the context of appropriate regulations to ensure data privacy and security.

Third, AI can be used to improve application security. AI can help find weaknesses in applications and fix security issues before they are exploited by attackers. AI can help to monitor and analyze app activity to detect potential attacks and threats. AI can also help to predict and prevent attacks by analyzing patterns of abnormal behavior and activity within the app. Using machine learning algorithms, AI can learn and identify patterns of behavior that can indicate unauthorized attacks or actions, such as searching for confidential data or hacking activity. AI can also help to prioritize cyber defense responses and actions by evaluating threat levels and potential losses. AI can be used to improve app security in ways such as; Authentication by verifying user identities and preventing unauthorized access by analyzing behavioral and biometric patterns, detecting attacks by monitoring application activity and

detecting attacks such as SQL injection, DDoS, and other attacks, and log analytics that utilize log analytics to detect unauthorized activity and aid in attack investigations.[24]

Competition between countries in the use of cyber to strengthen defense systems (*defensive objectives*) and the manufacture *of cyber weapons* (*offensive objectives*) is increasing. Moreover, a new technology called *Artificial Intelligence* (AI) has emerged today. AI is a technology that is able to provide analysis and solutions to protect organizations from cyberattacks and prevent more complex problems from occurring by effectively analyzing millions of cyber anomalies. For this reason, AI is increasingly integrated into cybersecurity structures and is used in various problems to automate work or support the tasks of security teams.[25]

AI can be used to create simulations and training in a variety of models used to train troops with various combat systems. To this end, AI is combined with *augmented reality* (AR) and *virtual reality* (VR) technologies to create virtual environments that resemble real situations. Nevertheless, the use of AI has also raised concerns in military contexts. An example is the development of autonomous weapons that can select and attack targets without human supervision. Although the development of this kind of weapon takes a long time, AI has begun to be integrated with existing military platforms, such as drones that work in groups and kamikaze drones. In addition, AI can also be used in the development of autonomous tanks, advanced missiles, and in battlefield healthcare such as evacuation and remote surgery. In this case, machine learning and AI can help in medical diagnosis and treatment of injuries in the midst of war situations.

AI can also be used for threat monitoring in the context of defense. This activity involves network monitoring, by analyzing, evaluating, and monitoring organizations and network *endpoints* to prevent the entry of ransomware, intrusion, malware, and the like.[26] *Machine learning algorithms* can be trained to detect malware, recognize patterns, and detect ransomware attacks before they enter the system. AI is also playing an important role in the development of intelligent systems to increase awareness of threats, especially those installed

[24] Ishak Farid. et al, The Utilization of Artificial Intelligence in Cyber Defense, NUSANTARA: Journal of Social Sciences, Vol 10 No 2 of 2023 p. : 779-788

[25] Gunawan Wibisono, et al, Strategies for Improving the Capability of Cyber Units in Spam Through the Utilization of Artificial Intelligence in Cyber Security Based on the National Institute of Standards and Technology Cybersecurity Framework Version 1.1, Journal of Education and Teaching Review, Volume 7 Number 1, 2024

[26] Nur'adila, R. (2023). Security Trends Using Artificial Intelligence.

on UAVs. Countries such as the United States, Russia, China, India, and others use drones to detect threats, especially in remote areas.[27]

Today, the use of AI in defense mostly exists in six main areas, namely:

1. Weapon targeting and autonomous weapons, currently autonomous weapons platforms use computer vision to identify and track targets. Autonomous weapons primarily become autonomous when the system can identify, and track targets in space that has been deployed to guard. The artificial intelligence behind targeting needs to be trained on what exactly a viable strategic target is to focus its firepower on and inform operators monitoring the platform.
2. Surveillance (*intelligence, surveillance, reconnaissance*). AI is particularly useful in intelligence because of the large datasets available for analysis. For example, in the first phase of Project Maven involved automating intelligence processing to support counter-ISIL campaigns. Specifically, the Project Maven team combines computer vision and machine learning algorithms into an intelligence gathering cell that will comb through footage from unmanned aerial vehicles and automatically identify hostile activity for targeting.
3. Cybersecurity. Cybersecurity threats come in many shapes and sizes. Artificial intelligence or AI has the ability to play a huge role in preventive measures for a military. AI is likely to be a key technology in advancing operations and cybersecurity.
4. Homeland security. One of the core capabilities of artificial intelligence is to identify trends and patterns in data sets to then predict the likelihood and when those trends will occur again. This is called predictive analytics, and it is currently applied to homeland security issues.
5. Logistics. AI may have future uses in the field of military logistics. The U.S. Air Force, for example, is starting to use AI for predictive aircraft maintenance. Instead of making repairs when an aircraft breaks down or fits into a standard fleet-wide maintenance schedule, the U.S. Air Force is testing an AI-enabled approach that adjusts maintenance schedules to the needs of individual aircraft.

[27] Ferryma Arba Apriansyah, et al, Literature Review: Threat of Artificial Intelligence (AI) Cyber Attacks on Data Security, International Journal of Education, Information Technology and Others (IJEIT), April 20242, 7 (2), 54-63

6. Autonomous vehicles. Most countries are now seeking to incorporate AI into semi-autonomous and autonomous vehicles, including fighter aircraft, drones, ground vehicles, and naval vessels. AI applications in this field are similar to semi-autonomous commercial vehicles, which use AI technology to see the environment, recognize obstacles, fuse data sensors, plan navigation, and even communicate with other vehicles.[28]

[28] Roth, M. (2019, February 22). Artificial Intelligence in the Military – An Overview of Capabilities. Retrieved from Emerj: https://emerj.com/ai-sector-overviews/artificial-intelligence-in-the-military-an-overview-of-capabilities/

State Defense Efforts in Facing the Threat of Artificial Intelligence

The integration of AI technology, particularly in urban warfare scenarios, has sparked significant concern among observers. Despite its sophistication, AI lacks understanding of the Law of Armed Conflict, so its application in urban environments becomes particularly problematic. AI's narrow outlook further complicates its ability to deal with complex urban conflicts, raising concerns among experts about the emergence of "killer robots" in the combat fleet. The level of concern around the implementation is increasing.

AI has led organizations like *Human Rights Watch* to advocate limiting the use of AI in critical decision-making. They propose measures such as banning the use of biological and chemical weapons, which aim to reduce the potential dangers associated with fully automated AI systems. One of the main concerns is AI's vulnerability to hacking and malware infiltration, as happened with the Stuxnet cyber weapons incident a decade ago. The malware infiltrated the control software of a uranium enrichment facility in Iran, indicating potential catastrophic consequences.

Human Rights Watch emphasized the need for regulations that specifically target AI units that are fully autonomous and capable of making lethal decisions, deploying mines, and initiating chemical and biological attacks (Marr, 2021). The vulnerability of AI systems to hacking poses a significant risk, potentially leading to scenarios where machines are manipulated to act contrary to their intended directives. The possibility of a rebellion or a change of alliance by AI-controlled forces adds complexity and uncertainty to military operations.

The idea that machines are susceptible to external manipulation that is beyond human control raises deep ethical and strategic concerns.[29] While AI promises to improve efficiency and decision-making capabilities on the battlefield, the potential for unintended consequences and abuse requires careful consideration and regulatory scrutiny. Additionally, the ability to remotely change troop loyalty underscores the need for robust cybersecurity and protection measures to prevent unauthorized access and manipulation of AI systems. The

[29] Suhardi, Yunita, A., Marheni, Wardhani, R. S., Levany, Y., Rahmadoni, F., Fibrianto, A., Erwandy, Susanto, Maniah, & Martoyo, A. (2023). Fraud Risk Management. TOHAR MEDIA

possibility of adversaries exploiting vulnerabilities in AI technology for strategic advantage is a major challenge for military planners and policymakers.[30]

The use of AI in defense has had an impact on Indonesia's defense strategy. The evolution of Industry 4.0 characterized by AI, *machine learning*, *big data*, system integration, and robotics technology has contributed to the threat revolution in military technology, but it can be a non-military threat because it is used, among other things, to dominate markets that are detrimental to domestic interests. The infrastructure (means) used in dealing with AI threats in defense are tools with AI technology, either purchased or produced by themselves, including chips installed at the border, unmanned aircraft such as drones, and robotic sea drone ships. Meanwhile, in cyber defense, there is no use of AI, it is still being developed and it is expected to have sensors with AI capabilities, to help simplify and shorten analysis.

To achieve the desired goals in dealing with AI threats in defense and providing support for the security and defense of the State, the following ways/*measures* are needed:[31]

1. The making of various policies, laws and regulations that are adequate as a basis. In Presidential Regulation Number 8 of 2021 concerning the General Defense Policy for 2020-2045, it is discussed that the development of defense technology is directed to utilize AI. Then BPPT launched the Indonesian Artificial Intelligence National Strategy (Stranas KA) 2020-2045, which is a national policy direction in developing AI technology which is used as a guideline in the field of AI research operations in Indonesia for Ministries, organizations, local governments and other stakeholders. There is also the creation of short-, medium, and long-term strategic planning, which includes ensuring sufficient budget needs to deal with AI threats.
2. Strengthening intelligence capabilities to understand the development of AI threats and be able to overcome them. Determination of national vital objects that need to be secured from unmanned system / AI attacks. Strengthening the regional defense system and non-military sectors.

[30] Jonni Mahroza, Indonesia's Views on the Use of Artificial Intelligence for Military Purposes, NUSANTARA: Journal of Social Sciences, Vol 11 No 4 of 2024 p. : 1606-1612

[31] Azizah Nur Rahmatika, Indonesia's National Defense Strategy in Facing the Threat of Artificial Intelligence, Journal of Asymmetric Warfare Volume 8, Number 1 2022, 97-98.

3. Development of the domestic defense industry. Efforts are being made to develop an integrated and sustainable AI defense system by purchasing or procuring unmanned attack system barik anti-attack equipment from within the country and abroad.
4. Continuous recruitment and training of human resources. The lack and still lagging behind Indonesian technology, it's okay if we are not able to and cannot produce ourselves, we can buy with the note that there must be clauses for technology transfer, technology transfer, training so that we can be able to make our own.
5. Integrated power building between the main components, reserves and supports. A clear division of authority, duties, responsibilities and functions among State institutions/agencies in dealing with AI threats.
6. Conducting bilateral, multilateral cooperation at the regional and international levels. Collaborate and integrate in *a triple helix* (government, industry, academics), up to multiple helix in the development of national AI strength.

CONCLUSION

The results of the study show that;

1. The ITE Law as a positive law that applies in Indonesia groups AI into electronic systems and agents where if referring to the characteristics of AI from the definition of electronic systems contained in the ITE Law, there is a lot of harmony because AI has a way of working, one of which is collecting data and then processing it even to the analysis stage and has the ability to convey electronic information in accordance with what is contained in "Article 1 Number 5 of the ITE Law".
2. The use of AI in defense mostly exists in six main areas, namely; Weapons targeting and autonomous weapons, Surveillance (*intelligence, surveillance, reconnaissance*), Cybersecurity, Homeland security, Logistics, and Autonomous vehicles
3. To achieve the desired goals in dealing with AI threats in defense and providing support for the security and defense of the State, ways/measures are needed, including; The formulation of various policies, laws and regulations as an adequate basis, the strengthening of intelligence capabilities, the development of the domestic defense industry, the recruitment and training of sustainable human resources, the development of integrated forces among the main components, reserves and supporters, and the implementation of bilateral, multilateral cooperation at the regional and international levels.

BIBLIOGRAPHY

Abdul Hadi, Reform of National Law in Efforts to Protect Personal Data in the Era of Artificial Intelligence Disruption, Mimbar Justitia Law Journal, Vol. 8 No. 1 – June 2022

Anastasya Zalsabilla Hermawan, Literature Study: The Threat of Artificial Intelligence (AI) Cyber Attacks on Data Security in Indonesia, Proceedings of the 2023 National Seminar on Information Technology and Systems (SITASI) Surabaya, 6 – 7 September 2023

Ardian Yudopratomo, Challenges to the Future of National Defense Due to Artificial Intelligence, NUSANTARA: Journal of Social Sciences, 10 (8) (2023): 4051-4057

Azizah Nur Rahmatika, Indonesia's National Defense Strategy in Facing the Threat of Artificial Intelligence, Journal of Asymmetric Warfare Volume 8, Number 1 2022.

Caiming Zhang and Yang Lu, "Study on Artificial Intelligence: The State of the Art and Future Prospects," Journal of Industrial Information Integration 23, no. May (2021): 100224,

Corrigan, J. (2017, November 3). Three-Star General Wants AI in Every New Weapon System. Retrieved from. https://www.defenseone.com/technology /2017/11/three-star-general-wantsartificial-intelligence-every-new-weapon-system/142239/

Endang Purwaningsih & Irfan Islami, Analysis of Artificial Intelligence (Ai) as Inventors Based on Patent Law and Islamic Law, Galuh Justisi Scientific Journal, Volume 11 Number 1-March 2023

Farid Abdul, (2019), Digital Phenomena in the Era of the Industrial Revolution 4.0, Journal of DKV Dimensions of Fine Arts and Design, 4(1).

Ferryma Arba Apriansyah, et al, Literature Review: Threat of Artificial Intelligence (AI) Cyber Attacks on Data Security, International Journal of Education, Information Technology and Others (IJEIT), April 20242, 7 (2), 54-63

FL. Yudhi Priyo Amboro, & Khusuf Komarhan, The Prospect of Artificial Intelligence as a Subject of Civil Law in Indonesia, Law Review Volume XX, No. 2 – November 2021

Gunawan Wibisono, et al, Strategies for Improving the Capability of Cyber Units in Spam Through the Utilization of Artificial Intelligence in Cyber Security Based on the National Institute of Standards and Technology Cybersecurity Framework Version 1.1, Journal of Education and Teaching Review, Volume 7 Number 1, 2024

https://emerj.com/ai-sector-overviews/artificial-intelligence-in-the-military-an-overview-of-capabilities/

https://pendidikanmu.com/2018/11/pengertian-kecerdasan-buatan-menurut-para-ahli.html

Ishak Farid, et al, The Utilization of Artificial Intelligence in Cyber Defense, NUSANTARA: Journal of Social Sciences, 10 (2) (2023): 779-788

Jajang Nurzaman, et al, The Validity of Contracts Made by Artificial Intelligence According to Positive Law in Indonesia, Al' Adl: Journal of Law, Volume 16 Number 1, January 2024.

Jonni Mahroza, Indonesia's Views on the Use of Artificial Intelligence for Military Purposes, NUSANTARA: Journal of Social Sciences, Vol 11 No 4 of 2024 p. : 1606-1612

Makarim, E. (2018). Indonesian Legal Framework for Cybersecurity. Retrieved from. http://www.nisc.go.jp/security-site/campaign/%20ajsympo/pdf/lecture2.pdf

Margaret A Goralski and Tay Keong, "The International Journal of Arti Fi Cial Intelligence and Sustainable Development" 18, no. June 2019 (2020)

Marufah, N., Rahmat, H.K. and Widana, I.D.K.K., 2020. Moral Degradation as the Impact of Cybercrime on the Millennial Generation in Indonesia. NUSANTARA: Journal of Social Sciences, 7(1), pp.191-201.

Muhammad Tan Abdul Rahman Haris & Tantimin, Analysis of Criminal Law Liability for the Utilization of Artificial Intelligence in Indonesia, JOURNAL OF LEGAL COMMUNICATION, VOLUME 8 NUMBER 1 FEBRUARY 2022

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

Ni Made Yordha Ayu Astiti, Strict Liability of Artificial Intelligence: Accountability to AI Regulators or Is AI Given the Burden of Accountability?, Udayana Master Law Journal, Vol. 12 No.4 December 2023, 962-980

Nur'adila, R. (2023). Security Trends Using Artificial Intelligence.

Paulus Wisnu Yudoprakoso, Artificial Intelligence as a Tool to Assist the Law Drafting Process in an Effort to Face the Industrial Revolution 4.0 in Indonesia, Indonesian Law Symposium Volume 1 Number 1 of 2019

Ronny Hanitidjo Soemitro, Law and the Development of Science and Technology in Society, Inauguration Speech of Permanent Professor at the Faculty of Law, Diponegoro University, Semarang, December 6, 1990.

Roth, M. (2019, February 22). Artificial Intelligence in the Military – An Overview of Capabilities. Retrieved from Emerj:

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

Suhardi, Yunita, A., Marheni, Wardhani, R. S., Levany, Y., Rahmadoni, F., Fibrianto, A., Erwandy, Susanto, Maniah, & Martoyo, A. (2023). Fraud Risk Management. TOHAR MEDIA

Tippe, S. (2016). Defense Science: History, Concept and Implementation. Jakarta: Salemba Humanika

Widodo Budiharto and Derwin Suhartono, 2014, Artificial Intelligence: Concept and Application, Andi Publishers, Yogyakarta

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