RSTDE
Remote Sensing Technology in Defense and Environment
RSTDE 1(2): 86–97
ISSN 3062-8970

Institute for Advanced Science, Social and Sustainable Future
MORALITY BEFORE KNOWLEDGE

Anticipating the impact of artificial intelligence to increase national vigilance against terrorism attacks in Indonesia

Ilmiawan Muhammad Bahriansyah[1,*], Asep Adang Supriyadi[2], Poppy Setiawati Nurisnaeny[1]

[1] *Intelligence Studies, National Intelligence College, Bogor, West Java 16810, Indonesia;*
[2] *Sensing Technology, Faculty of Science and Technology, Republic of Indonesia Defense University, Bogor, West Java 16810, Indonesia.*
*Correspondence: aadangsupriyadi@gmail.com

Received Date: May 30, 2024 Revised Date: July 30, 2024 Accepted Date: August 30, 2024

ABSTRACT

Background: The rapid advancement of artificial intelligence (AI) poses significant challenges to national security, particularly in the context of cyber terrorism. Indonesia, as a country with a large Muslim population and a history of terrorist activities, faces unique threats that could exploit AI technologies for malicious purposes. The increasing frequency of cyber attacks, including botnet attacks and malware incidents, highlights the urgent need for comprehensive strategies to counter these threats. **Methods**: This study employs a literature review methodology, analyzing relevant academic articles, policy documents, and case studies on AI and cyber terrorism. The analysis focuses on the intersection of AI technologies and terrorism, exploring the vulnerabilities within Indonesia's cyber security landscape and examining international cooperation frameworks aimed at combating cyber threats. Data sources include scholarly journals, government reports, and publications from international organizations. **Findings**: The findings reveal that Indonesia's current cyber security infrastructure is inadequate to handle the evolving threats posed by AI-driven cyber terrorism. Notable vulnerabilities were identified in critical sectors, including government and financial institutions, exacerbated by previous cyber breaches. Furthermore, the study highlights the potential use of AI in advanced weaponry, such as kamikaze drones, which could significantly impact national security. **Conclusion**: To mitigate the risks associated with AI-based cyber terrorism, Indonesia must enhance its legal frameworks and foster international cooperation. Effective measures include harmonizing national laws with international standards and strengthening collaborative efforts with regional partners. Such initiatives are crucial for developing a robust defense against the multifaceted challenges of cyber threats. **Novelty/Originality of this article**: This study contributes to the existing literature by providing a comprehensive analysis of the implications of AI for cyber terrorism in Indonesia. It underscores the importance of integrating international legal instruments with national policies, offering a novel perspective on addressing the vulnerabilities within Indonesia's cyber security framework. The emphasis on regional cooperation and the exploration of innovative counter-terrorism strategies further enhance the originality of this research.

KEYWORDS: artificial intelligence; cyber terrorism; cyber security; kamikaze drones; national security.

1. Introduction

The probability of technological development today is very complex where technology plays an important role in the use of individuals, companies or organizations for certain situations and contexts. The existence of Artificial intelligence is currently one of the technological developments that have received global attention due to the progressive

Cite This Article:
Bahriansyah, I, M., Supriyadi, A, A., & Nurisnaeny, P, S. (2024). Anticipating the impact of artificial intelligence to increase national vigilance against terrorism attacks in Indonesia. *Remote Sensing Technology in Defense and Environment*, 1(2), 86-97. https://doi.org/.....

nature of automation in solving problems faced by humans in every aspect of life. Technology is essentially a double-edged spear, especially with regard to aspects of national security where one side can help a country strengthen and maintain the stability of its national security, but on the other hand it is also a supporting factor for the realization of dangers that threaten the security of a country, especially the phenomenon of terrorism, which is closely related to technological developments (Nadjia, 2023). One of the national security threats posed by terrorism activities in the cyber world is targeting losses in the global economy where this practice has been felt by countries such as China, Australia, Russia, Ukraine, India and the United States which often get anomalous cyber attacks from radical extremists and cyber criminals using AI and Malware virus capabilities (Capuano, 2016). America, which often get anomalous cyber attacks from radical extremists and cyber criminals using AI capabilities and virus malware (Capuano, 2016). In connection with this, it is necessary to have a breakthrough or a way to deal with the phenomenon of using AI in an anti-terrorism and radicalism approach where the group sophisticatedly utilizes cyberspace or internet-based cyberspace or a very complex program base in order to transform destructive goals against certain instruments in a country.

Deepening the intentions of terrorists in using the purity of technology that was originally to help humans in all respects but turned it into harming humans in all respects, it is necessary to dissect the meaning of terrorism activities, namely a movement that uses violence or the threat of violence in order to achieve certain political interests, certain religious interests, the imposition of certain ideologies carried out by non-government groups in order to create a climate of fear of terror (Saidi, 2022). The intimidation method on the aspect of violence repeated by underground groups with the aim on the religious or political spectrum as a step to create the essence of fear for certain groups and society at large (Schimd, 2023). The concept of terror psychology theory by A.P Schimd explains that in the position of a terrorist where the victim of terrorism seems to be only a spark of enthusiasm for terrorism to achieve its main goal of influencing, intimidating, forcing, impressing or influencing one or more other groups or briefly called by creating terror in the form of systematic threats to make the target helpless. In practice, terrorists also often manipulate individuals or larger organizations such as the government in responding to acts of terrorism, which sometimes consider terrorism as an ordinary crime or a strategic systematic act.

The effect of the cyberspace phenomenon on the dynamics of terrorism activities is the birth of a cyber terrorism movement with a vision and mission to create a climate of fear and cyberspace instability in a country. Cyber terrorism is one of the most difficult crimes to handle from the perspective of law, politics, socio-culture, economy, military or technology due to its complexity or the nature of terrorism operations in a cross-cultural scope complexity or the nature of terrorism operations in a transcontinental and cross-border scope against certain geographical and geopolitical conditions. As a result, national security becomes very vulnerable to attacks where the location of the attack is specific or random with sources of damage that are difficult to measure using conventional technology and law enforcement.

2. Methods

The writing method for this literature study research is carried out with a systematic approach to identify, evaluate, and analyze various relevant sources of information related to the threat of Artificial Intelligence (AI)-based cyber terrorism in Indonesia. The initial process began with a literature search through academic databases. The keywords used included “cyber terrorism,” “artificial intelligence,” “cyber security,” and “international cooperation.” The sources obtained were then screened based on inclusion criteria, such as relevant, recent, and peer-reviewed publications. In this way, we ensured that the information used had high validity and reliability.

Next, qualitative analysis was applied to evaluate the content of the selected literature. This approach involves in-depth reading of each source, noting key points, and identifying key themes that emerge in the literature. From this analysis, the author developed a categorization based on aspects related to the threat of cyber terrorism and its prevention strategies. This process also involved comparing the views of various authors regarding the effectiveness of different approaches in addressing this issue. In this way, the author was able to identify gaps in existing research and propose further research directions. The research follows a clear structure, starting from the introduction that describes the background of the research to the conclusion that presents the findings and recommendations. Each section is arranged logically to facilitate the reader's understanding and present the information in an organized manner. References are included with appropriate citation formats, such as APA or MLA, to give credit to the original sources and ensure academic integrity. Through this systematic approach, it is expected that the research results can make a significant contribution to the development of cybersecurity policies and practices in Indonesia. The research flow of thought can be seen in Figure 1.

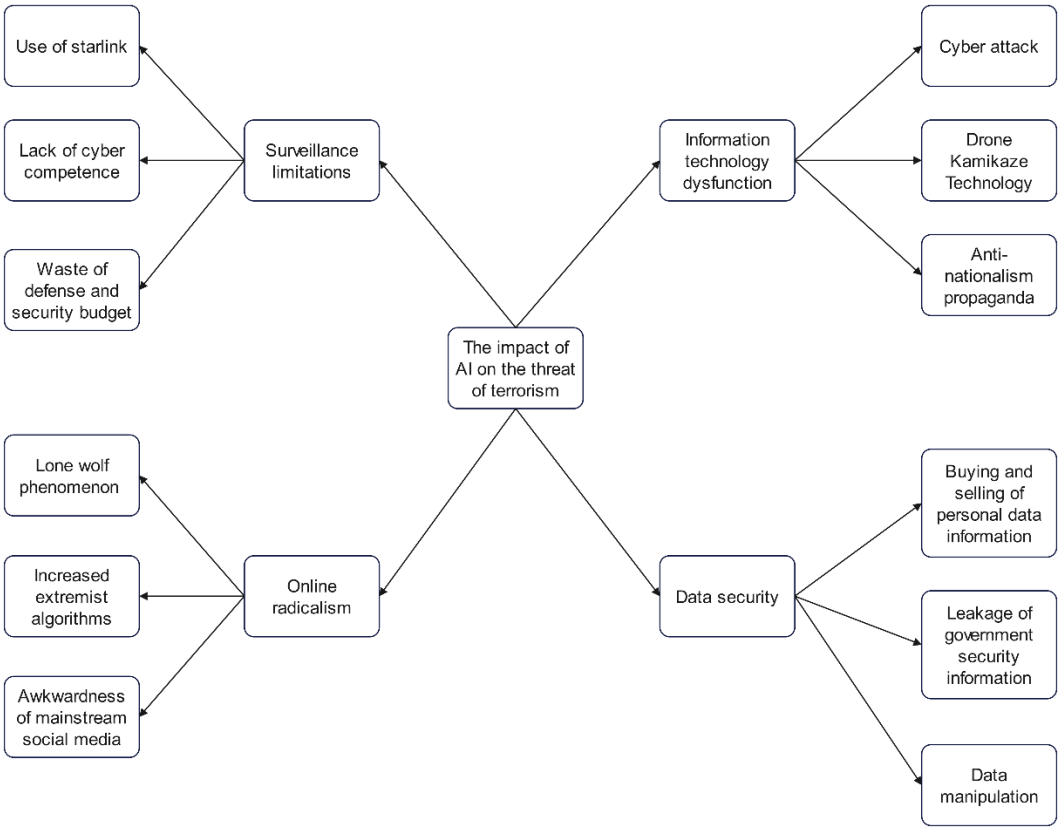

Figure 1. The research flow

3. Results and Discussion

3.1 Probability of potential cyber terrorism threats in Indonesia

Terrorism capabilities in cyberspace are characterized by obscuring sources of information that can be used by a country's security forces in conducting systematic tracking of threat sources. This is related to the complexity of the closed nature of the internet by using extra encryption features for sensitive data and information used by terror actors in order to support planning and operations. At another level, the nature of the common practice of terrorism, namely the loss of human life, has a huge impact on the security conditions of each country where this impact targets economic conditions comprehensively on the structure of investment, production and other economic capacities

of a country (Bardwell, 2020). The vulnerability of state interests to the impact of terrorism activities is very vulnerable when viewed from any strategic perspective such as politics, economics, security, socio-culture and so on so that the main focus of the state's role in dealing with this phenomenon is national stability using the functions of security and intelligence instruments (Telford, 2020). Generally, it is very difficult for a country's security forces to correlate any physical evidence obtained such as traditional crime cases due to the competency factor in the cyber technology space. This is because terror actors have very high competence, disinformation, differences in time and place, the application of applicable laws in each country, and the commitment to eradicate terrorism, especially in cyber space.

Vulnerability to radicalism and terrorism activities in the cyber sphere can be felt by every country without exception, especially Indonesia where the use of computational automation work systems and dependence on the internet has been carried out in every line of life in Indonesia. The use of technology in cyberspace in Indonesia is widely used in important infrastructure sectors such as finance, public transportation, defense and security, politics, health and society, as well as social and cultural, so how vulnerable Indonesia's national security is if there is a cyber attack by terrorists in a systematic and complex manner. Cyber attacks using AI automation will certainly have a major impact on terrorism activities in Indonesia where the characteristics of cyber terror are low cost with a high level of effectiveness and an extraordinary level of attack mobility where conventional terrorism uses violent instruments such as the use of firearms, and explosives but with the implications of AI-based terrorism with attacks carried out using only computer and internet instruments.

Cyber terrorism generally operates in a calm environment and does not require significant violence such as the use of weapons which only requires computers and internet network systems to carry out cyber breaches or cyber attacks whose effects are more destructive such as damage to a country's electrical installations or internet shutdowns (Rosanti, 2021). Isis or the Islamic state of Iraq and Syria and Al-Qaeda are among the terrorism actors that use cyberspace and AI automation in their operations such as information gathering operations, recruitment operations, attack planning, coordinating fighters, financing aspects or state actors who use elements of cyber terror in order to attack the national security of other countries as happened in the Russia-Ukraine war (Shandler, 2021). The relevance of using AI technology in a series of terrorism attacks is based on the accessibility of the internet which is very holistic, broad and comprehensive so that it can be used by anyone who has competence towards or in other words, every individual or group and even countries that have goals or perspectives in line with terror operations within the scope of ideology or certain issues will use this conception.

This factor is rooted in the interconnectedness of psychological aspects experienced by individuals or groups, especially marginalized youth in developing countries, who face challenges in political, economic and ideological aspects. This situation often leads to feelings of loss of meaning in life, triggered by legal injustice, economic inequality, unemployment, poverty, and other social discrimination. According to Nadjia (2023), some of the main variables that contribute to the emergence of cyber terrorism activities include hatred towards society due to experiences of injustice and rights violations; media influences that trigger hatred and a spirit of revenge; and the absence of the role of a person, family, or society in fulfilling basic human psychological needs such as attention and affection, which causes individuals to lose a sense of love and loyalty to the homeland. In addition, developing countries also often face an identity crisis due to dependence on global culture, which raises the potential for cultural conflict in the social structure of society, as is felt in some parts of Indonesia. Finally, misunderstandings in interpreting religion and social values, often resulting from ignorance of the actual religious laws or complex sectarian interpretations, contribute to radical or extremist actions.

Political factors often trigger cyber terrorism activities, especially through interstate conflicts that lead to cyber operations to damage other countries' critical systems. For example, the United States once conducted cyber terrorism operations against Cuba to

condition Cuba not to interfere with American national interests and weaken the influence of the Soviet Union during the Cold War era (Hegghammer, 2023). Other factors that support the occurrence of cyber terrorism in the political context include the absence of geographical boundaries in cyberspace that allows terrorism using AI technology, weak cyber technology defenses of the targeted country, lack of technological supervision from the target government, and the absence of comprehensive laws to regulate cyber crime, making it easier for cyber terrorism to launch attacks on the national interests of the target country. These factors appear to have triggered a number of cyberattacks in Indonesia, resulting in significant disruptions in Indonesia's political, socio-cultural, security, and cyberspace sovereignty.

From a technical perspective, developing countries face major obstacles as they generally lack specialized technological instruments, such as AI-based supercomputers, to anticipate cyberattacks. This allows terrorists to utilize AI in dangerous operations, such as the use of suicide drones, while drone countermeasure technology is still very minimal, especially in Indonesia. In addition, network security structures in developing countries tend to be weak and highly dependent on network defenses from developed countries, which opens a gap for developed countries to take advantage of these weaknesses and intervene, including by using cyber terrorism approaches that utilize encryption that is difficult to unravel by the technology of developing countries such as Indonesia.

3.2 Potential threat of AI modules in terrorism operations in Indonesia

Every latest technological advancement or commonly referred to as the era of IoT (Internet of Things) can open up new opportunities and applications in various aspects of life such as the birth of recon drone technology or commonly referred to as Reconnaissance Unmanned Aerial Vehicle (RUAV), Autonomous Weapons like Kamikaze Drones and Unmanned combat aerial systems (UCASs), Bio Hack, Autonomous Bio Weapon and Chip War. These technological developments basically play in the area of defense and security of a country and are indeed supporting instruments in geostrategic and geopolitical positions in the global 5.0 era. However, like a double-edged sword where the development of this technology becomes a threat gap for a country. The concept of the threat posed is the use of this technology for the strength and operation of terrorism in a country. These advances are essentially a challenge to adaptability, consistency in terms of security, and moral norms and rules of use due to the biased nature of technology affecting human psychology. For example, the birth of drone technology that has multipurpose capabilities can even be useful as a medium of intimidation against security stability that threatens human security and safety, as evidenced by the birth of suicide drones in various war events today (Jore, 2020). With the progressive development of technology, various aspects of deterrence are needed to anticipate the potential use of this technology in negative areas such as acts of general criminality or terrorism.

To understand more about AI-based technologies that can be used in acts of terrorism, one of them is autonomous drone technology. In the era of globalization, the use of drones has grown rapidly in various aspects of life, especially in the field of defense and security. Drones, which are equipped with autonomous systems and high-mobility microchips, are capable of operating at an altitude of around 200 feet and are integrated with complex systems that allow an operational range ranging from tens to tens of kilometers. This technology is used in military missions, such as reconnaissance, aerial monitoring and data collection. Drones themselves have several types of operating systems, namely: drones with manual pilot control on the ground, drones with remote control that function independently but can be supervised by humans, and fully autonomous drones that operate without human intervention (Husodo, 2020). In addition to military aspects, drones are also utilized in various civilian sectors, such as disaster management and monitoring, exploration and rescue, tourism development, commercial applications, crime surveillance, logistics, environmental management, and exploration of underwater natural resources (Noh, 2019).

The popularity of drone technology has increasingly attracted military and security attention in many countries, especially given its use in warfare, such as in the Russia-Ukraine conflict, and by ISIS for acts of terror in Iraq and Syria (Azhar, 2023). This phenomenon has the potential to pose a similar threat to other countries, including Indonesia, which still faces radicalism and terrorism in its society. Although drones bring benefits in various fields, this technology also poses security threats, both physical and cyber, especially when used in restricted areas or in extreme cases for bomb attacks. Some of the emerging threats include: weaponized drones used in terror operations against specific targets; suicide drones carrying explosives to attack targets directly; the risk of mid-air collisions that could threaten civil aviation; signal jamming that damages communications and jeopardizes critical infrastructure such as aviation and power; illegal access to networks through backdoor or key-logging methods; and illegal smuggling of prohibited items, including explosives or weapons, across borders (Azhar, 2023). These threats emphasize the importance of strict oversight and regulation of the use of drone technology in maintaining national security in the digital era.

Regarding the popularity of drones in their use in society, especially in the field of weaponry, developed countries have now developed drones that will be used specifically in the field of defense where the United States has developed the UVsion 120 barcode drone kamikaze technology, then Israel with Sky Striker products and Turkey with Alpagu Fixed Wing products are a series of technologies developed specifically for AI-based operations so that in operation it can select targets and attack trajectories. This drone model with AI is very, very potential to be a threat in all acts of terrorism both carried out by an organization and a state actor because until now anti-drone technology that can operate 100% has not been found. Indonesia, in this case, needs to take definite steps to prepare for this phenomenon of drone warfare considering that anti-drone technology in Indonesia is still very common and would certainly be a real threat if terrorism groups use drone systems with AI mechanisms to operate in large-scale terrorism attacks against government targets or the public at large.

Bioterrorism using AI systems is a new threat mechanism in the world of technological development where the nature of terrorism bureaus that use biological instruments such as pathogens, fungi, viruses and toxins that are generated and deliberately released into certain environmental structures with the aim of destroying certain sources of life quickly or slowly. The nature of bioterrorism is initially an impact of the development of biotechnology, synthetic biology and agricultural biotechnology in the context of modernizing systems in biological and chemical sciences but over time it is used as an important instrument in defense and security (Broeders, 2023). In practice, large private companies use biotechnology as a tool to mutate new types of viruses that can be marketed or released as biological weapons so that they can threaten certain governments or as a bargain position for personal gain (Liden, 2023). The background of the emergence of this bio weapon begins with the development of agricultural technology commonly known as Agri Tech which is a branch of biotechnology that uses scientific tools and techniques in order to modify tissue culture, genetic engineering and vaccination in plants, plants, microbes and animals. The impact of this biotech application causes environmental pollution such as food barns, water sources, causing several diseases for humans. This is utilized by several private companies and multinational corporations with state sponsorship using the BioTech impact mechanism as a biological weapon to create chaos in a certain area and as bargaining power in the geopolitical aspect.

The use of bioterrorism technology has occurred in Kenya from 1952 to 2015 where terrorism attacks were strongly indicated as tactic bioterrorism where in 1952 there was a mass death of livestock known as the “mau-mau” tragedy followed by the emergence of mass rift valley fever in 1997 and several years later there were many cases of cholera virus spread and the emergence of the maize mosaic virus which paralyzed maize production in Kenya in 2012 (Bala, 2021). Technically, the application of AI technology in bioterrorism focuses on producing terror pathogens that can cause various diseases for animals and even humans, such as Ebola, Bubonic Plague bacteria, Tularemia bacteria, Influenza viruses,

smallpox, encephalitis viruses by mosquitoes, dengue viruses, botulinum toxin bacteria and various bacterial or viral modifications by AI mechanisms (Helbling, 2020). Some models of bioterrorism technology that can be a threat are Anthrax/Smallpox which can be used as a biological weapon by terrorism to transmit diseases quickly and accurately and efficiently where the nature of anthrax disease is easier to modify in any laboratory so that it can be bred as a model of biological weapons that are no less effective than bombs or artillery.

In the mechanism of the spread of anthrax biological weapons begins with the spread of spores in a certain area with an incubation period of 5-7 days. In addition, exposure to the skin will enter the human or animal digestive system so that it can spread secretly into the body until a serious impact occurs for infected humans or animals because it can stop the body's organ work system (Broeders, 2023). Historically, the use of biological weapons has been used several decades such as during the 6th century BC the Assyrians poisoned enemy wells with fungi that made the enemy dizzy and confused, in 1336 the Mongol army's attempt to infect city dwellers in what is now Ukraine by throwing the corpses of bubonic plague victims over the city walls and in 1763 according to British military reports that a British officer planned to deliberately transmit smallpox to Native Americans during the Pontiac rebellion near fort Pitt or the Pittsburgh region. In the World War 2 era, Japan also used plague as a biological weapon during the Sino-Japanese war where by filling bombs with parasites and dropping them over Chinese cities and using cholera and shigella pathogens as weapons in several attacks that killed around 580,000 Chinese people due to Japanese biological weapons (Chukwuma, 2022). The threat of bioterrorism is actually a more real threat compared to the terror of Nuclear weapons due to the greater likelihood of occurrence. Indeed, the absence of a concrete blue print on how to prevent bioterrorism attacks globally makes every mechanism of bioterrorism attacks increasingly complex in attack methods and impacts.

Although, the attack using bioterrorism has not actually been in a large or massive attack area as predicted by US defense experts in the era of the Iraq war, it is said that the country's government has the ability to attack using biological weapons of mass destruction and later it was not proven. However, the scale that occurs in biological attacks in several places and times in the small category but makes it increasingly difficult for security parties globally to track the pattern of attacks and subsequent attack mechanisms due to the complexity of biological weapons. At another level, the popularity of bioterrorism weapons is a serious threat that uses the biological mechanism of action of microorganisms and toxins intentionally derived from plants, animals, microbes and so on to produce diseases with the aim of causing human death with the media for the distribution of biological weapons using penamun materials of various sizes such as simple glass bottles, handbags, backpacks, suitcases or even wallets and pocket pockets (Does, 2019).

A real potential threat arises if biological weapons are used in acts of terrorism in a country, especially due to the relatively easy access to these resources, the lack of detection by security systems, and the low cost of production. Indonesia needs to take proactive steps for early detection and prevention against possible bioterrorism attacks in its territory, through legal arrangements and operational standards as implemented in the United States. Following the anthrax attacks in 2001, the United States introduced bioterrorism and public health security preparedness and response legislation as a strategic measure to deal with bioterrorism threats and natural disasters. The implementation of these laws includes preparedness of every government structure and social community, control of chemical and biological materials to prevent misuse as weapons, and interagency coordination to monitor hazardous materials. In addition, improving health infrastructure, such as integrated laboratories, vaccination rooms, and quarantine centers, is a priority, along with building an integrated early warning system at the government level and the wider community so that vigilance against the threat of biological weapons can be increased.

For several decades, terrorism in Indonesia has experienced ups and downs due to factors such as the massive and progressive use of technology that facilitates terrorism operations in Indonesia. Terrorism in Indonesia has a very complex network and is global in nature so that holistically it will affect the conduciveness of global security considering

Indonesia's largest Muslim population globally. Reflecting on the Bali Bombing II incident which shook the world, especially the United States and its western allies, strategic steps need to be taken to condition Indonesia to remain proportionally stable while maintaining the interests of western countries in Indonesia. One form of prevention is used in the mechanism of laws related to agreements formed by international organizations that provide a concrete basic concept for exercising universal jurisdiction over cyberspace, especially in the field of terrorism, implemented and established through the international community and the state. Cyber terrorism is an activity that is cross-state and cross-legal in nature, which essentially requires an international approach in order to respond to threats due to the concept of attacks carried out by cyber terrorism using AI in anyone and any country (Vega, 2020).

Multilateral cooperation is an effective approach in responding to transnational cybercrime, given that each country has different regulations regarding computer crime, legal aid, and other substantive laws (Kuhl, 2022). One of the main organizations playing a role in this effort is the Executive Directorate of the UN's Committee on Counter-Terrorism (CTED), which supports global efforts against terrorism, including cyber threats involving artificial intelligence (AI). CTED provides technical support and strengthens global communications, and encourages countries to punish perpetrators of cyber terrorism. On the other hand, the Vienna International Counter-Terrorism Convention also focuses on strengthening the international legal framework to prevent the use of advanced technologies such as AI in the nuclear and radioactive sectors for acts of terrorism. The International Organization of Telecommunications (ITU), a specialized unit of the UN, aims to protect global critical infrastructure through emergency network strengthening and information technology security cooperation at the international level.

Interpol, through its Cyber Fusion Centre located in Singapore, plays a significant role in combating cyber terrorism by collecting and analyzing intelligence on global cyber threats. The team identifies terrorist groups that use AI technology and their recruitment and attack patterns. Interpol also has a special team called the Incident Response Team that is ready to assist countries that are victims of cyber attacks in dealing with the immediate impact of the attack. In addition, the Council of Europe Convention on Cybercrime is the first international legal instrument to focus on cybercrime as a whole, covering offenses such as illegal access, data interference, and misuse of devices. It provides a framework for the comprehensive investigation of cybercrime, which now also includes countering AI-based cyber terrorism.

Other initiatives include IMPACT, a global collaboration that aims to facilitate cooperation between governments, the private sector, academia, and international organizations in addressing cyber threats. Based in Cyberjaya, Malaysia, IMPACT serves as a global hub for information and strategies in dealing with cyber threats, especially related to critical infrastructure such as financial systems, power grids, and nuclear power plants (Galaz, 2021). In the Asia-Pacific region, APEC also played an important role through the telecommunications and information ministerial statement on information and communications infrastructure security. APEC encourages its member economies to implement comprehensive legislation related to cybersecurity and cybercrime based on agreed international legal instruments (Prah, 2021).

Indonesia can also play the role of international cooperation, especially in the regional area, in order to prevent early forms of AI threats in terrorism activities considering that the existing terrorism cells in Indonesia have not been eliminated completely. Regional powers and cooperation such as ASEAN, can be used by Indonesia in order to combat all forms of AI dysfunction in cybercrime, especially terrorism, as outlined in the ASEAN regional security cooperation forum. One of the cooperation forums formed such as the 4th seminar on cyber terrorism scheduled at the ASEAN Ministerial meetings in the discussion of transnational crimes issued a declaration to make substantial improvements to the legal framework for handling crimes related to the use of computers and integrated partnerships with Interpol and UN anti-terrorism agencies (Hogetoorn, 2020). In fact, there is no general approach to countering cyber terrorism using automation mechanisms such as AI because

cyber terrorism cases are transnational, so only international consensus can be used as a strategic step (Schuurman, 2019). Why anti-terrorism cooperation measures are needed in the face of the fight against terrorism activities that use AI automation mechanisms, because currently there is no proportional and long-term anti-AI technology and multiverse in the face of technological developments and AI versions. So, to catch up with the development of these technologies, other strategies that are more effective and efficient are needed, such as forming international cooperation with other countries so that they can help each other in the mechanism of preventing criminal acts of terrorism in cyberspace.

4. Conclusions

Artificial Intelligence is an important aspect of the industrial revolution in a country with significant impacts on several crucial things such as defense and security aspects. Some studies explain that the threat of AI is quite real affecting the security situation of a country where cyber attacks often occur in several countries such as AI Botnet attacks with the mechanism of attacking a country's computer infrastructure. Attacks using malware to computers and their networks will have an impact on criminal acts such as extortion, data theft and can even be used as terrorism operations in a country. Indonesia's weakness in the data security system strengthens the vulnerability of this cyber attack considering that there have been several breaches of Indonesia's cyber security system by many parties ranging from small groups to groups sponsored by other countries. Cases that have occurred such as the breach of the cyber security system of Indonesian government websites such as Kominfo, local governments, and several private parties such as Tokopedia, and the break-in of several state-owned banks make the potential threat of cyber terrorism attacks very likely.

At another level, the threat position of using renewable technology that can be converted with AI mechanisms such as multipurpose drones, needs to be of particular concern to the security and intelligence apparatus in Indonesia. This is because, recently, the use of drones in warfare events such as the Russian and Ukrainian wars and Israel and Hamas used Drone Kamikaze technology or suicide drones as a very effective weapon instrument. The concept of kamikaze drones is considered very powerful in carrying out sporadic attacks and effective in destroying certain points in various contours of the geographical environment. It is likely that if the Kamikaze Drone technology does not become an important issue at the international level, anyone will easily create, modify and produce this dangerous instrument. If the terrorist groups in Indonesia study seriously and comprehensively this kamikaze or suicide drone device easily and cheaply, it will certainly be used in a series of attacks on government facilities and the public in general.

At another level, there are many AI technologies that can threaten Indonesia's national security in addition to the potential threat from the use of Kamikaze Drones, namely AI drones for Jamming, biohacking systems, bio weapons which can all be developed and operated with AI mechanisms that can have a very destructive, complex and very difficult impact to prevent with conventional legal, political and technological approaches. The most important essence in preventing potential terrorism attacks using AI bases can occur, namely international cooperation both in the regional and regional scope. This is because there are no countries globally that are able to fend off cyber attacks, especially acts of terrorism with existing cyber infrastructure. This is because the nature of cyber attacks is multidimensional, cross-border, outside the legal boundaries of a country, and clashes of interests between countries so that the basic concept of countering and preventing terrorism does not run effectively. So concrete steps are needed as an effort to respond to the potential threat of cyber terrorism in the field of AI such as the need for internal harmonization of draft laws related to cybercrime to support Law number 11 of 2008 concerning ITE by combining national legal instruments with international legal instruments for the effectiveness of the implementation impact of binding regulations and bargaining power of national interests.

Author Contribution
The author contributed fully to the research.

Funding
This research did not receive funding from anywhere.

Ethical Review Board Statement
Not applicable.

Informed Consent Statement
Not applicable.

Data Availability Statement
Not applicable.

Conflicts of Interest
The authors declare no conflict of interest.

References

Azhar, Z. (2023). Kesiapan teknologi kamikaze drone untuk peperangan modern di Indonesia. *Teknik Mesin dan Mekantronika, Vol. 8* , NO. 1, 1-8.

Bala, B., & Tar, U. (2021). Regional cooperation in west africa: counter-terrorism and counter-insurgency. *African Security, Vol. 14*, No 2, 186-207. https://doi.org/10.1080/19392206.2021.1929747

Bardwell, H., & Iqbal, M. (2020). The Economic Impact of Terrorism from 2000 to 2018. *DE GRUYTER*, 227-261. https://doi.org/10.1515/peps-2020-0031

Broeders, D., Cristiano, F., & Weggemans, D. (2023). Too close for comfort: cyber terrorism and information security across national policies and international diplomacy. *Studies in conflict & terrorism, vol. 46,* no 12, 2426-2453. https://doi.org/10.1080/1057610X.2021.1928887

Capuano, N. (2017). Explainable Artificial Intelligence In Cybersecurity: A Survey. *IEEE Access, Vol. 4*. https://doi.org/10.1109/ACCESS.2022.3204171

Chukwuma, K. H. (2022). Critical Terrorism studies and postcolonialism: constructing ungoverned spaces in counter-terrorism discourse in nigeria. *Critical studies on terrorism, Vol. 15*, NO 2, 399-416. https://doi.org/10.1080/17539153.2022.2048990

Does, R. V., Kantorowicz, J., Kuipers, S., & Liem, M. (2019). Does terrorism dominate citizens hearts or minds? the relationship between fear of terrorism and trust in government. *Terrorism and political violence, Vol. 00*, 1-18. https://doi.org/10.1080/09546553.2019.1608951

Galaz, V., Centeno, M., Callahan, P., Causevic, A., Patterson, T., & Brass, I. (2021). Artifical Intelligence, Systemic risks. *Technology in society*. https://doi.org/10.1016/j.techsoc.2021.101741

Hegghammer, T., & Ketchley, N. (2023). Plots, Attacks, And The Measurement of Terrorism. *Journal of Conflict Resolution, Vol.* 1-27. https://doi.org/10.1177/00220027231221536

Helbling, M., & Meierrieks, D. (2020). Terrorism and Migration, an Overview. *British Journal of Political Science*, 1-20. https://doi.org/10.1017/S0007123420000587

Hogetoorn, B. (2020). The Impact of terrorism on international mergers and acquisitions: evidence from firm-level decisions. *Peace Research*, 1-16. https://sagepub.com/journals-permissions

Husodo, A. Y., Jati, G., Octavian, A., & Jatmiko , W. (2020). Switching target communication strategy for optimizing multiple pursuer dronse performance in immobilizing kamikaze multiple evader drones. *ICT Express, Vol. 6* , 76-82. https://doi.org/10.1016/j.icte.2020.03.007

Jore, S. h. (2023). Is Resilience a Good Concept In Terrorism Research? A Conceptual Adequacy Analysis of Terrorism Resilience. *Studien In Conflict % Terrorism, Vol. 46*. No 1-20. https://doi.org/10.1080/1057610X.2020.1738681

Kühl, N., Schemmer, M., Goutier, M., & Satzger, G. (2022). Artificial intelligence and machine learning. *Electronic Markets, 32*(4), 2235-2244. https://doi.org/10.1007/s12525-022-00598-0

Liden, K. (2023). A Better Foundation For National Security. *Cooperation and Conflict, Vol. 58* . 3-22. https://doi.org/10.1177/00108367211068877

Nadjia, M. (2023). The Role Of Artifical Intelligence in Combating Cyber Terrorism. *IUS ET SCIENTIA, Vol. 9* . http://doi.org/10.12795/IESTSCIENTIA.2023.i02.10

Noh, J., Kwon, Y., Son, Y., & Shin, H. (2019). Tractor Beam: safe-hijacking of consumer drones with adaptive GPS spoofing. *ACM Transaction on privacy and security, Vol. 22*. https://doi.org/10.1145/3309735

Prah, P. K., & Chanimbe, T. (2021). Ghana's readiness to combat terrorism: strategi of security institutions. *the international journal of intelligence, security and public affairs, Vol. 23*, NO, 3, 367-399. https://doi.org/10.1080/23800992.2021.1968582

Rosanti, D., Nurmandi Achmad, Muallidin, I., & Kurniawan, D. (2021). Meta-Analysis At The Root Terrorism From The Perspective of Islamic Movement In Indonesia. *Jurnal Hukum dan Pranata Sosial*, 393-420. https://doi.org/10.19105/al-lhkam.v16i2.4817

Saidi, F. (2022). A Hybrid Deep Learning-based framework for future terrorist activities modeling and prediction. *Egytian Informatics Journal*, 437-446. https://doi.org/10.1016/j.eij.2022.04.001

Schuurman, B. (2019). Topics in terrorism research: reviewing trends and gaps, 2007-2016. *Critical studies on terrorism, Vol. 12,* no 3, 463-480. https://doi.org/10.1080/17539153.2019.1579777

Shandler, R., Gross, M. L., Bachaus, S., & Canetti, D. (2021). Cyber Terrorism and Public Support For Retaliation - A Multi-Country Survey Experiment. *British Journal Of Political Science,* 1-19. https://doi.org/10.1017/S0007123420000812

Telford, A. (2020). A Climate Terrorism Assemblage ? Exploring The Politics Of Climate Change-Terrorism-Radicalisation Relations. *Political Geography, 79*. https://doi.org/10.1016/j.polgeo.2020.102150

Vega, R. P., Kaartemo, V., Lages, C. R., Razavi, N. B., & Mannisto, J. (2020). Reshaping the contexts of online customer engagement behavior via artificial intelligence: a conceptual framework. *Journal of Business Research*. https://doi.org/10.1016/j.jbusres.2020.11.002

Biographies of Author(s)

Ilmiawan Muhammad Bahriansyah, Intelligence Studies, National Intelligence College.
- Email:
- ORCID:
- Web of Science ResearcherID:
- Scopus Author ID:
- Homepage:

Asep Adang Supriyadi, Sensing Technology, Faculty of Science and Technology, Republic of Indonesia Defense University.
- Email: aadangsupriyadi@gmail.com
- ORCID: https://orcid.org/0000-0003-1103-6669
- Web of Science ResearcherID:
- Scopus Author ID: 57201546735
- Homepage:

Poppy Setiawati Nurisnaeny, Intelligence Studies, National Intelligence College.
- Email: poppy@stin.ac.id
- ORCID: https://orcid.org/0000-0003-0531-0019
- Web of Science ResearcherID:
- Scopus Author ID: 57222902846
- Homepage: