Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 15s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

The State's Responsibility Towards Citizens For Criminal Acts Of Transnational Terrorism In The Form Of Cyber Terrorism Through New Media

Made Wishnu Adi Saputra[1], Mella Ismelina Farma Rahayu[2]

[1,2]Faculty of Law, Tarumanagara University, Indonesia

Email ID: wisnuadsptr@gmail.com, Email ID: mellaismelina@yahoo.com

Cite this paper as: Made Wishnu Adi Saputra, Mella Ismelina Farma Rahayu, (2025) The State's Responsibility Towards Citizens For Criminal Acts Of Transnational Terrorism In The Form Of Cyber Terrorism Through New Media. *Journal of Neonatal Surgery*, 14 (15s), 581-595.

ABSTRACT

This research analyzes the state's responsibility in dealing with criminal acts of transnational terrorism committed through cyberterrorism using new media. Indonesia, as a sovereign country, has the responsibility to maintain national security and contribute to global security as mandated in the 1945 Constitution of the Republic of Indonesia. Terrorism, especially in the form of cyberterrorism, poses a significant threat that requires serious action and a strong legal response. Cyberterrorism is the use of information and communication technology to carry out terrorist attacks that cause physical, psychological or economic damage. This phenomenon requires countries to increase their cyber capacity to detect and prevent these attacks. In the context of international law, state obligations regarding terrorism are regulated by the UN and various international conventions, such as the 1999 International Convention for the Suppression of the Financing of Terrorism. States are responsible for preventing, punishing, and providing reparations for victims of terrorism. In a national perspective, the Law of Indonesian Terrorism emphasizes that the state must provide medical assistance, psychosocial rehabilitation, and compensation to victims. This research finds that terrorism is a global threat that requires a strong legal response from the state, both in the national and international context. Countries must also develop a comprehensive legal framework to deal with cyber terrorism and ensure protection for victims. This research is expected to contribute to the development of effective policies and laws in dealing with the threat of transnational terrorism and cyberterrorism, as well as increasing protection for citizens.

Keywords: *Transnational terrorism, Cyber terrorism, State responsibility.*

1. INTRODUCTION

Indonesia as a sovereign country has a responsibility to maintain the security of its citizens and contribute to global security. This is mandated in the Preamble to the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945), which states that the Indonesian State protects the entire Indonesian nation and all of Indonesia's blood and promotes general welfare, makes the life of the nation intelligent, and participates in implementing world order based on independence. , lasting peace, and social justice.

The crime of terrorism is a form of crime that has an international dimension because the various acts of terror carried out have created fear in society and claimed many victims in various countries in the world (Schmid, 2011). International conventions such as the Convention for the Prevention and Punishment of Terrorism (1937), the International Convention for the Suppression of Terrorist Bombings (1998), and the International Convention for the Suppression of the Financing of Terrorism (1999), have categorized terrorism as a transnational crime. Terrorism is not only an extraordinary crime but also requires handling with extraordinary measures.

According to Kurtulus (2017), terrorism is defined as the use of violence to cause fear in order to achieve goals, especially political goals. The Indonesian Ulema Council also defines terrorism as an act of crime against humanity and civilization that poses a serious threat to state sovereignty, world security and social welfare (Suharto, 2020).

In Indonesia, several terrorist incidents such as the Bali Bombing Tragedy in 2002 which killed 184 people and injured more than 300 people, show how serious the threat of terrorism is.(Syihab & Hatta, 2023). Other incidents include the Christmas bombings in 2000 and the explosions at the Ritz Carlton and JW Marriot hotels in 2009. These acts of terror show that the terrorist movement is one of the biggest threats to security and humanity, both in Indonesia and in the world.

Transnational terrorism can be carried out by foreigners in Indonesia or Indonesian citizens abroad Hambali, a terrorist involved in several major attacks in Southeast Asia, is an example of a case of transnational terrorism. He played a role in the bombings in various cities in Indonesia on Christmas Eve 2000, the Philippine Embassy Bombing on August 1, 2000, and the Bali Bombings in 2002 (Al Qurtuby, 2022; Chandler & Gunaratna, 2007). Hambali is also considered a liaison between Jemaah Islamiyah and Al-Qaeda.

Along with technological developments, terrorism has also transformed into a more sophisticated form, namely cyber terrorism. Cyber terrorism is the use of information and communication technology to carry out terrorist attacks. Yadav (2022) defines cyber terrorism as unlawful acts and threats of attacks on computers, networks and information stored therein which are carried out to intimidate or coerce governments or people in supporting political or social goals. CRS Report for Congress in (Kronstadt & Vaughn, 2004; Kuru, 2023) also stated that cyber terrorism is the use of computers as weapons or targets by politically motivated international or sub-national groups or secret agents who threaten or cause violence and fear to influence society or cause the government to change its policies.

This research is based on several basic questions that need to be answered to understand and overcome the issue of transnational terrorism, especially in the form of cyber terrorism that uses new media. First, it is important to explore the nature and meaning of criminal acts of terrorism as regulated in national and international law. Terrorism is a complex and dynamic crime, the definition of which can vary depending on the legal framework used. Therefore, this analysis will help understand how national and international law defines and categorizes criminal acts of terrorism.

Second, this research needs to answer the state's responsibilities in dealing with criminal acts of transnational terrorism. It includes international and national legal perspectives, looking at how states are responsible for preventing and addressing acts of terrorism involving more than one state. This responsibility includes prevention, action, and recovery for victims, all of which are regulated in various international conventions and agreements.

Third, focus on the concept of state responsibility towards citizens involved in criminal acts of transnational terrorism, especially in the form of cyber terrorism that uses new media. Information and communication technology has changed the way terrorism is carried out and countered. Therefore, it is important to understand how countries can and should act in the face of this growing threat.

This research aims to analyze and discover the essence and meaning of criminal acts of terrorism based on national and international law. This is important to provide a comprehensive understanding of the definition and characteristics of terrorism in various legal frameworks. In addition, this research aims to analyze and discover state responsibility for criminal acts of transnational terrorism. This includes the state's legal and moral obligations in preventing and tackling terrorism as well as providing protection and reparations for victims.

Furthermore, this research also aims to analyze and discover the concept of state responsibility towards citizens involved in criminal acts of transnational terrorism, especially in the form of cyber terrorism through new media. This will help formulate effective policies in dealing with these threats and ensure that countries are able to protect their citizens from cyber attacks.

It is hoped that the results of this research will provide theoretical and practical benefits. Theoretically, this research can be useful for the development of criminal law science, especially in relation to the state's responsibility in dealing with criminal acts of transnational terrorism. Apart from that, this research can be additional reading or relevant literature regarding transnational criminal acts in the form of cyber terrorism using new media.

Practically, it is hoped that this research can provide input for the government to establish international cooperation in dealing with criminal acts of transnational terrorism. This can also be input for legislators in initiating more specific regulations regarding the state's responsibility towards citizens who commit terrorism abroad. In addition, the results of this research can be used by other researchers who want to explore similar topics.

The concepts used in this research include responsibility, state, terrorism, cyber terrorism, and new media. The state's responsibility for criminal acts of transnational terrorism includes legal and moral obligations to protect its citizens and take effective preventive and enforcement steps. Hans Kelsen (2019) divides responsibility into four categories: individual, collective, fault-based, and absolute.

The state as a sovereign entity has the authority to make and enforce laws and protect citizens from internal and external threats. Jellinek in Wahjono (2009) also Fraser (2020) defines the state as an organization of power that obtains legitimacy from society and has a certain territory.

Terrorism is an act of violence committed to achieve political, ideological, or religious goals by causing fear in society. According to Law Number 15 of 2003, terrorism is defined as the use of violence or threats of violence that causes an atmosphere of widespread terror or fear.

Cyber terrorism is the use of information technology to carry out terrorist attacks. Saul (2021) defines cyber terrorism as an unlawful act that threatens or attacks computer systems and networks with the aim of intimidating or coercing the government or society.

New media is media that uses digital technology and the internet to communicate and disseminate information. According to McQuail (2010), new media has the characteristics of interactivity, accessibility, and flexibility that enable two-way communication between users.

This research uses several theories as a basis for analyzing the problems raised. The rule of law theory is used to discuss the legal status of criminal acts of terrorism based on national and international law. According to Dicey in (Muhlashin, 2021) said that the rule of law emphasizes that state power must be exercised based on fair laws and provide benefits to society.

Responsibility theory is used to analyze the state's obligations in preventing and handling criminal acts of transnational terrorism. According to Kelsen in (Satino, Yuli, Surahmad, & Andriyanto, 2023), legal responsibility includes the state's obligation to enforce the law and provide reparations to victims.

Cyberterrorism theory is used to analyze the use of information technology in carrying out terrorist attacks. Denning (2000) explains that cyberterrorism involves the use of computers and networks to cause physical, psychological or economic damage.

2. METHOD

This research uses a juridical method normative, which emphasizes the analysis of applicable legal norms. This method was chosen because this research aims to analyze the state's responsibility for criminal acts of transnational terrorism in the form of cyberterrorism through new media based on national and international law. This normative juridical approach provides an in-depth understanding of how the law regulates and responds to these issues (Shidarta, 2020).

This research began with collecting secondary data consisting of primary, secondary, and tertiary legal materials. Primary legal materials include national legislation such as Law Number 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism and various international conventions such as the International Convention for the Suppression of Terrorist Bombings (1998) and the International Convention for the Suppression of the Financing of Terrorism (1999) (Komalasari, 2011). Secondary legal materials include literature, legal journals, and scientific articles that provide analysis and interpretation of primary legal materials. Meanwhile, tertiary legal materials consist of legal dictionaries and encyclopedias that support an understanding of the legal concepts used in this research.(Shidarta, 2020).

Data analysis in this research was carried out using a qualitative approach which allows researchers to understand and interpret the meaning of the data that has been collected. The first step in this analysis is to carry out an inventory and classification of data based on topics that are relevant to the research problem formulation. The data that has been classified is then analyzed using relevant legal theories to answer the research questions.

To answer the first question regarding the nature and meaning of criminal acts of terrorism based on national and international law, this research analyzes the definitions, characteristics, and elements that make up criminal acts of terrorism in various laws and regulations and international conventions. This analysis is carried out by comparing various definitions and elements to find similarities and differences (Adji, 2017; Ridwan, Suhar, Ulum, & Muhammad, 2021).

The second question regarding the state's responsibility in dealing with criminal acts of transnational terrorism is analyzed by looking at the legal obligations regulated in various international conventions and national legislation. This research also examines how these obligations are implemented in practice by countries involved in handling cases of transnational terrorism (Chandler & Gunaratna, 2007; Vita Indah, 2021).

To answer the third question regarding the concept of state responsibility towards citizens involved in criminal acts of transnational terrorism in the form of cyber terrorism through new media, this research analyzes how information and communication technology is used in committing criminal acts of terrorism and how the law responds to this development. This analysis also involves case studies of cyber terrorism attacks that occurred in various countries to understand attack patterns and legal responses to them (Denning, 2000; Kronstadt & Vaughn, 2004).

This research also uses a comparative approach to compare the regulations and policies implemented in various countries in dealing with criminal acts of transnational terrorism and cyber terrorism. This approach helps in identifying best practices that Indonesia can adopt to strengthen its legal and policy framework in dealing with these threats (Chandler & Gunaratna, 2007; Yuliana & Hasibuan, 2022).

In analyzing the data, this research pays attention to legal principles that apply internationally and nationally, as well as relevant legal theories such as rule of law theory, responsibility theory, and cyber terrorism theory. The theory of the rule of law is used to discuss how the law regulates state actions in dealing with criminal acts of terrorism (Saputra, Sinaulan, & Farhana, 2023). The theory of responsibility is used to analyze the state's obligations in preventing and handling criminal acts of terrorism, as well as providing reparations to victims (Ampriyanto & others, 2018). Meanwhile, cyber terrorism theory is used to understand the dynamics of the use of information technology in carrying out terrorist attacks and how the law responds to these threats (Denning, 2000).

By using normative juridical methods, this research is expected to provide a comprehensive and in-depth analysis of state

responsibility for criminal acts of transnational terrorism in the form of cyberterrorism through new media. It is also hoped that this research can provide relevant and applicable recommendations to strengthen the legal and policy framework in dealing with the threat of terrorism increasingly complex and dynamic.

3. RESULTS AND DISCUSSION

Facts about Terrorist Movements

The terrorist movement in the 21st century has received serious attention by most countries in the world. After the devastating terrorist attacks nine years ago on the WTC (World Trade Center) twin buildings in New York, the Pentagon and the White House in the United States (US) on September 11 2001, as well as successful and failed terrorist bomb attacks towards countries in various parts of the world, including in the Southeast Asia region such as the Philippines, Singapore, Thailand and Indonesia. Specifically for Indonesia, the most devastating terrorist attack occurred on October 12 2002 when two nightclubs, namely, Sari Club and Paddy's located in Kuta, Bali were bombed by the Jemaah Islamiah (JI) terrorist network which caused the death of more than 200 people, the victims were not only Indonesian citizens but also foreign citizens, especially Australians.

The problem of terrorism and the war against terrorism is a big challenge for the post-cold war world. Even though it can be said that terrorism is not a new problem, but rather a problem that has existed for decades and even centuries, terrorism has become a frightening global threat since the early years of the end of the cold war. Governments, both in developed and developing countries, and even in underdeveloped countries, or in countries that have been established or are in turmoil or unstable and are identified as "failed states", are not immune from the threat of emerging movements and actions. - acts of terrorism on an international scale. Globalization, which has been taking place rapidly recently, has made it easier for ideas and actions to unite to resist the world system through movements and acts of international terrorism.

After Al-Qaeda, the international terrorist organization which is considered a serious threat to world security is the Islamic State of Iraq and Syria (ISIS). The organization led by Abu Bakr Al-Baghdadi has controlled several regions in Iraq and Syria, and also has an extensive network with jihadist activists in Islamic countries, both in the Middle East and Asia. In Indonesia, ISIS also has a network of former DI/TII, NII, JII, MMI, ATI followers from Ustadz Abdullah Sungkar and Ustadz Abu Bakar Ba'ashir. They have appointed Chep Ernawan as Chairman of ISIS Indonesia. Chep has the duty and responsibility to mobilize jihad in Iraq and Syria from Indonesian Muslims. Chep, a man from Cilacap, Central Java, recognizes Abu Bakr Al-Baghdadi as the caliph of the Islamic Khilafah Daulah who has religious, political and military authority for the world's Muslims. . Chep argued that Abu Bakr was a descendant of the Qurasy who was steadfast in jihad, had high enthusiasm and zeal in implementing Islamic sharia, and had a good track record. ISIS activists openly via YouTube invite Indonesian Muslims to join ISIS, and challenge the TNI to fight on the battlefield. ISIS's actions have created new unrest and a new threat of terrorism for Indonesian Muslims. The actions and reactions of Islamic mass organizations strongly oppose the presence and existence of ISIS Indonesia. MUI, NU, Muhammadiyah and other Islamic mass organizations, stand at the forefront of opposing ISIS's ideological penetration and acts of terrorism. This new transnational Islamic movement is a "real threat" to the integrity of the Unitary State of the Republic of Indonesia (NKRI).

The governments of the United States and Australia issued travel warnings to their citizens not to travel to Indonesia, considering the threat of ISIS terrorism. Of course, the travel warnings from these two countries have clearly caused political and economic losses to Indonesia. Therefore, TNI General Moeldoko's threat to destroy ISIS, if it does anything wrong in Indonesia, is very appropriate. This strong statement is a form of the TNI's determination to act decisively against ISIS, and a message to the world that Indonesia is very serious about tackling terrorism in Indonesia.

Terror and terrorists come suddenly and are always surprising, both for the public and the security forces. Terrorist target areas are also very diverse, including national capitals, important places or installations, tourist areas and so on. Therefore, Bali as a tourist area also has the potential for terrorist acts to occur again. As stated by the Commander of the Udayana IX Military Command after commemorating the 50th anniversary of the Udayana IX Regional Military Command in 2007, he said that the Island of the Gods still has the potential for terrorist threats. Therefore, he appealed to be wary of anyone coming and going, including local and foreign tourists who come to Bali. Bali security is special because Bali is a destination for international tourist visits. So, don't be careless. Moreover, there were two repeated bomb incidents in Kuta. Nowadays, anyone should be suspected, whether local or foreign immigrants. The greatest potential vulnerability to this threat comes through land and sea entrances. According to Commander IX Udayana, guarding Bali is not as easy as other areas. The reason is that the Island of the Gods has become the international spotlight. When Bali is hit by an incident, the impact is widespread and affects tourism.

As stated in the Preamble to the 1945 Constitution of the Republic of Indonesia, it is emphasized that one of the goals of the Republic of Indonesia is to protect the entire Indonesian nation and all of Indonesia's bloodshed. This means that the state (government) must take maximum action to protect the lives of citizens from all threats that endanger the lives of these citizens, one of these threats is acts or movements of terrorism which are latent threats or can suddenly threaten society.

It is also confirmed in Article 1 paragraph 3 of the 1945 Constitution of the Republic of Indonesia after the amendment states

that: The Indonesian state is a legal state. In the context of Indonesia as a state of law and its relationship with the state's goal of protecting the entire Indonesian nation and all of Indonesia's blood, especially protection from the threat of terrorist movements, it is natural for the state (government) to create legal norms (legislation) that regulate preventing and dealing with acts of terrorism.

Acts of terrorism not only have a national dimension, but also an international dimension. The crime of terrorism is a form of crime with an international dimension that is very frightening to the public. In various countries in the world, there have been crimes of terrorism, both in developed and developing countries, the acts of terror that have been carried out have caused many victims. Indonesia, as a country that is committed to maintaining world security and order, has implemented international cooperation with various countries in preventing and dealing with acts of terrorism. Including ratifying (ratifying) international agreements in the field of preventing and controlling acts of terrorism to be transformed into Indonesian national law.

Terrorism observer Wawan Purwanto stated that terrorism is an endless threat to Indonesia. This is because the terrorist incidents that occurred in Indonesia were proven to have been controlled by elements of foreign powers who had certain interests. On the other hand, Abdul Wahid Cs stated that the crime of terrorism is a crime which is a tragedy of human rights (Human Rights) considering the characteristics of this crime as a threat to identity, honor, dignity and human rights. For example, the Bali I bombing at the Sari Club and Paddy's Club Kuta, is a terror that deserves to be classified as the biggest crime against humanity in Indonesia with a large number of victims, namely around 200 people and carried out very cruelly.

In almost the same vein, FH Winata stated that terrorism is an extraordinary crime because the number of victims is so large, it is carried out suddenly, does not differentiate between targets, it can happen at any time and anywhere. Meanwhile, Humprey Wangke in his research report stated that based on intelligence reports there was indeed Al Qaeda involvement in Southeast Asia. This is because the Southeast Asia region is inhabited by no less than 210 million people who are Muslim. Even in the three ASEAN member countries, namely Indonesia, Malaysia, and Brunei, the majority of the population is Muslim. Under these conditions, Southeast Asia can become fertile ground for the development of Al Qaeda and a safe hiding place for its members who are targeted by security officials.

Cyber Theory Modus Operandi

Terrorists in committing cyberterrorism crimes have different modes of operation. Because the internet can be exploited easily, terrorist organizations have various ways to carry out these criminal acts. Terrorist organizations such as ISIS utilize the internet to help them realize their goals. ISIS creates and utilizes hacker organizations to make it easier for them to carry out cyberterrorism crimes. ISIS is assisted by the Cyber Caliphate Army (CCA); Sons Caliphate Army (SCA) Kalashnikov ESecurity Team; United Cyber Caliphate; The Islamic State Hacking Division (ISHD); Islamic Cyber Army (ICA); The group Rabitat AL-Ansar; and Cyber Rox Team (CTR). Based on the various activities carried out by the hacker organization, it can be seen that the modus operandi used by ISIS in carrying out the crime of Cyber terrorism, namely by carrying out Cyber attacks in the form of hacking, propaganda, fraud to obtain funding, Distributed Denial of Service (DDoS) attacks and Malware attacks.

To understand how the perpetrators of cyberterrorism work, here are several important things to pay attention to. First, the perpetrators of cyberterrorism are mostly terrorists. Andrew Michael Colarik emphasized that "there is no cyber terrorism without terrorism". This statement emphasizes that the perpetrators of cyberterrorism are terrorists. They carry out their terror activities using cyber facilities. The use of computers as a tool and target of attack is a form of use of violence and intimidation, especially for certain political purposes.

Second, The tools used are computer networks. The perpetrator or group of perpetrators carries out massive attacks to penetrate computer security networks (eliminate or disable important functions). The main targets are important infrastructure, such as public health, emergency services, government, defense industrial base, information and telecommunication, banking and finance, transportation, etc.

Third,According to Phillip W. Brunst, there are several general motivations why crimes are committed on the internet. Several factors become motivation, namely: location independence, speed, anonymity, internationality, and cost-benefit ratio. Brunst further explained that these five forms of motivation apply to cyber terrorism crimes or other ordinary cyber crimes. The differences can be known or observed in relation to the underlying agenda. The main goal of terrorists is to create fear, create economic panic or discriminate against political opponents. Other goals may be independent of the primary motive such as lowering monetary income or information gathering (either for conventional or electronic attacks).

Fourth,Terrorist attacks using internet media can be carried out at any time. The timing of the attack can also be done by taking advantage of the right momentum so that fear can spread widely among the community. In other words, the time of the attack will be correlated with the objectives, capabilities and vulnerability factors of the security system of the network that is used as the tool or target of the attack. For example, the situation of uncertain political turmoil has given this movement a place in carrying out acts of cyber terrorism. The situation of uncertain political turmoil is a momentum that is often exploited by cyber terrorism groups.

It cannot be denied that terrorism has penetrated people's lives. Like a virus, terrorism has spread for decades to various circles in the country. If previously, the spread used educational institutions and places of worship, now the presence of social media makes it easier to spread the virus of radicalism. The ideology of radicalism is instilled by terrorist groups through propaganda activities carried out in a closed and systematic manner, making it difficult for security forces to detect and prevent its spread. Apart from repressive measures by arresting suspected terrorists, preventive measures are crucial to stop its spread and restore those exposed to this ideology.

The modus operandi of terrorism propaganda, which was previously conventional, has been abandoned and evolved to take advantage of technological developments, especially the internet in social media, which is part of cyberterrorism activities. The most effective way to track their whereabouts in spreading terrorist propaganda using social media is of course to monitor these movements on social media which is widely spread on cyberspace / the Internet.

Technological advances have changed the way information is conveyed in society. Moreover, today information technology has become increasingly easier and cheaper. So that more and more terrorism propaganda via the internet is discovered. The current trend is that the spread of cyberterism content in the form of multimedia and writing is starting to be seen as a propaganda method. Where previously books, magazines, cassettes and videos containing propaganda had originally been in physical form, they had been uploaded to websites, blogs and social media to be distributed widely/massively and without limits/borderless.

In fact, it is not surprising that the internet, as a medium for exchanging information and communication, is also used by terrorists to spread propaganda. Remembering that historically the internet was initially developed for military purposes. The history of the Internet begins with the development of electronic computers in the 1950s. The initial concept of packet networking came from several computer science laboratories in the United States, England, and France. The American Department of Defense awarded contracts in the early 1960s for packet networking systems, including the development of ARPANET (which would be the first network to use internet protocols). The first message was sent via ARPANET from Computer Science Professor Leonard Kleinrock's laboratory at the University of California, Los Angeles (UCLA) to a second network node at the Stanford Research Institute (SRI). Where computers can be connected to each other globally so that each computer is able to offer access to programs and data. This research (distributed computer networks) is intended for military purposes. So the DNA of the internet itself actually flows and contains military DNA so that it is very possible to adopt it into activities to win a battle such as a military operation by acts of terrorism in instilling an understanding of their propaganda. Because terrorists can effectively use cyberspace for secure communication.

1. Propaganda

Propaganda or propaganda in Latin, which originally meant "to spread/improve/breed", has shifted in meaning to "an activity to spread a culture or ideology". According to the Big Indonesian Dictionary, Propaganda is defined as true or false information (beliefs, opinions, etc.) that is developed to convince people to adhere to a particular school, attitude or direction of action: usually accompanied by grandiose promises. Propaganda is defined as broadcasting opinions (political views and so on) to seek followers or support.

In identifying propaganda, there are important principles such as efforts to change public views. Changing views is carried out by influencing the emotional aspects of individuals en masse. Propaganda aims to establish similarities in beliefs, behavior and habits of the masses who are the target of propaganda.

The content of propaganda material depends on the goals that the spreader wants to achieve. For example, in a state of war, propaganda is aimed at influencing people and determining attitudes: patriotism, family life, hatred, confidence in ultimate victory, sense of courage, want to go on an adventure (sense of adventure), so that the war launched by propagandists gets support from the public.

Propaganda is not always active in promoting an ideology, sometimes propaganda is carried out by censoring other or foreign views. For example, censoring and excommunicating the views of Galileo and Copernicus about "the earth revolves around the sun" to protect the doctrine of "the sun revolves around the earth" so that Propaganda is very different from education even though the aim is to change views. Education teaches individuals "how to think", while propaganda "what to think". Propaganda proposes a discourse to the masses and closes down the possibility of criticism.

The spread of propaganda is a manipulative and dogmatic process where there is no room for criticism and developing alternative discourse. It is hoped that the masses who are the targets of propaganda will be emotionally influenced and devoid of rational thinking, so that they simply follow the discourse put forward by the communicator.

Techniques for spreading propaganda according to the Institute of Propaganda Analysis (IOPA), include:

The Use of Glittering Generalities

The Use of Glittering Generalities technique utilizes slogans, phrases or abstract sentences that are not specific. Slogans, phrases or sentences are designed in such a way as to attract people's attention. The Use of the Glittering Generalities technique is often found and used in political campaigns, such as calls for: "for the sake of justice", "voice of the people" or

radical propaganda such as, "for the establishment of the caliphate". Slogans like this are very charming and move the hearts of potential voters who are longing for justice, but it is not explained how to achieve the implementation of this slogan.

Name Calling

Name calling technique is propaganda used to demean the opponent/enemy, so that the opponent/enemy appears evil, stupid or has no abilities. In practice, name calling techniques are often used by terrorists to spread propaganda in Indonesia, where the term taghut is often used to undermine the credibility of the legitimate government. According to terrorists, taghut is considered an army of Satan to interpret law enforcement officials, while the government is considered an unjust and infidel government. Thaghut or tagut in Indonesian means that which is worshiped by people other than God.

Transfer

Transfer Techniques use means to build or destroy a reputation. In this technique, a speaker associates himself with other parties who have high credibility, so that the speaker appears to have a good reputation. For example, by associating someone with a charity movement to build a reputation (image). This person needs to be seen as caring and sensitive towards groups in need, so that society becomes more sympathetic. On the other hand, to destroy, a person is associated with other parties who are considered to have low credibility by society. For example, terrorists accuse the government and non-governmental organizations active in countering terrorism of being "foreign compradors".

Testimonials

This testimonial technique relies on a person's image or predicate, such as a famous person or someone who is considered an expert. By giving a positive statement about something, for example, the greatness of a political candidate, it is hoped that people will sympathize. In terrorism propaganda, a person who is held hostage by a terrorist group can also hysterically convey his testimony via video about the violence he has experienced or will experience, the goals of the terrorist group and the ransom desired by the terrorist group. The manipulation that occurs in this type of propaganda cannot be verified whether the expert giving the testimony really knows the candidate they are praising, it could be that they were paid to carry out the testimony, or it cannot be verified that the person giving the testimonial is a victim of being taken hostage by a terrorist group. In Indonesia, terrorist perpetrators provide testimonials through videos on the internet, letters and books.

The Plain Folks

The Plain Folks technique is manipulation to gain sympathy from the public by creating an image of ordinary people. With a simple appearance or a popular language style, it is hoped that society will evaluate someone as an equal and as part of society. An example is the book "Abu Bakar Ba'asyir Notes from Prison" which depicts the figure of Abu Bakar Ba'asyir as a simple religious figure.

Card Stacking

Card Stacking technique in propaganda, opening and promoting one issue while covering up other issues. Just like placing cards on the table, one side of the card will be open while the other side is closed. For example, in propaganda that promotes the privileges of an organization, its advantages compared to other organizations and the facilities obtained by members. With this incessant propaganda, it is hoped that other organizations will be denigrated by society. This can be seen from terrorism propaganda in inciting the public to take action against perpetrators of criminal acts of terrorism, where the perpetrators are made to look like good people who are treated unfairly by the police. On the one hand, it raises the image of terrorists, while also reducing the image of the police as law enforcement officers in the eyes of the public.

Bandwagon Technique

The Bandwagon Technique is based on the tradition of circus troupes in the 19th century in the United States. When a circus troupe enters a city, there will be a procession with music and cheers to attract the attention of the people, so that the people will be interested in buying tickets and watching the circus performance. Likewise, in this propaganda technique, a speaker or main communicator is shown directing an issue and encouraging people to follow his direction. This technique hopes that people will immediately follow. With the communicator's call, it is hoped that anxiety will arise if he does not immediately follow. This can be seen in the slogan "join immediately" or "your chance is only for today". This is what was done by the terrorist group which distributed a video inviting them to take part in paramilitary training in Aceh in 2010 as well as an ISIS propaganda video which was published on YouTube entitled "Join The Rank".

2. Propaganda Terrorism

Propaganda carried out by terrorism aims to promote acts of violence;

a. promoting extremist rhetoric that provides support for violence;
b. recruitment;
c. incitement;

d. radicalization.

One of the characteristics of terrorism propaganda is "Propaganda by deed". Propaganda by deed is a way of seeking public attention by conveying messages through violent means. Like the suicide bomb attacks carried out by terrorists, where the terrorist group wants the attention of the wider community for the attacks carried out, as well as spreading fear.

There are two commonly encountered models of Propaganda by Deed, namely:

a. *Propaganda by deed*carried out before the terror attack

As happened before the JW Marriot bombing in 2009. This propaganda by deed was carried out by Dani Dwi Permana, the suicide bomber in that incident. Propaganda by deed before the action can be in the form of a reason for carrying out a suicide bombing, or a testament to the family such as a review and apology to those closest to them, a message to certain groups to follow in their footsteps.

The message was delivered before the perpetrator carried out the suicide bombing with the aim of explaining to people that what the perpetrator did was solely to obtain justification. With propaganda like this, perpetrators hope to accept their actions, let alone imitate them. Even though killing oneself is something that cannot be justified in religious teachings, let alone killing other people.

b. *Propaganda by deed what* is done after the action

This propaganda conveys a message after the attack has been carried out. The goal is to strengthen the strength of the organization and seek support from certain groups. The perpetrator carried out a series of attacks on targets thought to be Thaghut in the hope of moving/awakening the people who saw his actions by blaming the government for forcing him to do this. This propaganda is characterized by using name-calling/inviting provocative words that attempt to undermine the government.

c. *Propaganda by Deeddone* during the action

This propaganda is carried out while a terrorist act is in progress, which can be carried out by the terrorists themselves or the mass media. For example, the terrorist attack on the WTC Twin Towers in the United States on September 11 2001 caused more than 2,000 casualties. The mass media, especially television, covered the process of the crash of a commercial plane, manned by civilians, into the twin buildings, repeatedly. Coverage of terrorist attacks causes extreme fear, not only for citizens of the United States but also around the world. Indirectly, the mass media plays a role in conveying terrorist messages through mass media, namely terror messages.

3. Propaganda Using Internet Facilities

By understanding propaganda that uses the spread of information to achieve its goals. So the internet media takes a very large and strategic portion and role for terrorist perpetrators in providing information to the public, especially young people about radical ideology as the aim of terrorist propaganda. The fact that terrorist organizations and those affiliated with them have utilized technology that makes it easier for them to spread propaganda so they can then recruit potential members via the internet is a very sad thing from the progress of mass media itself.

The internet is one of the most widely used and easiest media to channel propaganda. The internet has become a force for new media and political aspirations which according to Kahn and Kellner will become increasingly popular and entrenched in the future, where the growth of its users is rapid and difficult to predict and the variety of facilities provided to produce materials and models of democracy.

That there are more than 30 million internet users in Indonesia and the user growth rate is around 12.5 percent per year. Indonesia is also ranked 7th in the world in using Facebook, and currently there are at least 11,759,980 Facebook accounts created with the user age range between 18-34 years.

With this large number of users, it is inevitable that the internet will become a fertile virtual area for carrying out various political activities. It could be that the internet is a powerful medium for political movements in Indonesia. And it could also be that internet users emerge as a new force, pressure group, and virtual democratic mass base in upholding democracy in this country. The internet is no longer just a technological innovation in networking, but has transformed into a medium of political power.

Terrorism propaganda has also become a special concern of the United States intelligence agencies. George Tenet, Director of the Central Intelligence Agency (CIA) stated: “The new information technologies (IT) and the Internet are more often used by terrorist organizations in conducting their plans to raise the financial funds, distribute their propaganda and secure communications. The terrorist groups including Hezbollah's, Hamas and al-Qaeda, for support of their operations, use computerized files, e-mails and protection (encryption). The convicted terrorist Ramzi Yousef, the main planner of the attack on the World Trade Center in New York in encrypted files in his laptop computer stored detailed plans for aircraft destruction in the United States.”

Anticipation of activities for spreading propaganda by terrorism can be found in Article 43C of the Counter-Terrorism Law regarding Counter-radicalization. Counter-radicalization is a planned, integrated, systematic and continuous process carried out against people or groups of people who are vulnerable to being exposed to the radical ideology of Terrorism, which is intended to stop the spread of the radical ideology of Terrorism.

Propaganda carried out by terrorists is carried out through blogs published using their namesdescribes himself as a "freelance journalist" specializing in issues of Islamic society, with a focus on politics, strategy and intelligence. In his blog, Naim celebrates attacks carried out by ISIS-linked groups, and encourages and advises those who have pledged allegiance to the group. Many of the posts on his blog contain information on making explosives. In an article he praised an attack in Solo that he described as a "lone perpetrator, not linked to any terrorist network," to rise up against Indonesia. Apart from using blogs, terrorists also often use telegrams to provide instructions to their networks in carrying out terrorist activities that have occurred so far in Indonesia.

In carrying out propaganda using internet media, it is reported that the terrorist as the leader of the Katibah Nusantara militant group is said to be currently in Raqqa, Syria, the de facto capital of the Islamic State of Iraq and Syria (ISIS) after militants took control of it at the end of 2013. He carried out This act of propaganda and spreading the ideology of terrorism is aimed at offering encouragement and advice to those who have declared allegiance to militant groups and also explaining how easy it is to carry out jihad, or holy war, from "guerrilla warfare" in the Indonesian jungle to a city.

Propaganda and the spread of terrorist ideology via the internet is very dangerous and can influence the younger generation to be drawn into radical ideology of terrorism. To deal with the increase in the quality and quantity of terror attacks and propaganda, where currently there are still many gaps in Indonesia's positive laws that can provide space for the widespread use of the internet as a tool of terrorism, it is necessary to have a strategic formulation from the government in dealing with the phenomenon of using the internet for propaganda and dissemination activities. the ideology of terrorism in Indonesia so that it does not develop more widely.

The use of the internet as a means of communication and information continues to develop in people's lives. The internet was originally created to facilitate communication between academic and military circles connected to the Advanced Research Projects Agency Network (ARPANET) in 1969. Then it developed as a public service that was free to use for communication. However, this is experiencing a shift, the internet is being misused for criminal purposes6. Apart from crime, the internet is also used for terrorist purposes (internet use for terrorist purposes).

Apart from that, the most common misuse of the internet is the use of internet sites as a means of propaganda and spreading terrorist ideology. This condition must be a serious concern for the government to anticipate propaganda and the spread of terrorist ideology so that it does not further develop in Indonesia.

1. Propaganda

Although the practice of propaganda has occurred since the first formation of social society, the word propaganda only emerged when the Roman Church used propaganda as a means to spread the Catholic religion. In the following centuries, the role of propaganda shifted to its application in the world of politics as well as public relations and even the manipulation of public opinion. That is why, in every important event such as politics, elections, revolution, or war, propaganda provides a strong impetus for the development and practical implementation in the field of communication.

Etymologically, according to the Big Indonesian Dictionary, propaganda means information, understanding, attitude, or a certain direction of action, usually accompanied by grandiose promises. In Encyclopedia Britanica, 1997, and The Oxford Companion to the English Language, Tom Mc Arthur (1992: 333-334) explains that the word propaganda comes from the Neo Latin propagandus or propagare which means spread. This word was first used by Pope Gregory Since then, the word propaganda has begun to be widely used to refer to a systematic plan and organized movement to spread a particular belief, dogma, doctrine or system of principles.

Theoretically, propaganda messages should be repeated. Repetition techniques are very important and are basic in propaganda activities. Judging from its history, propaganda theory has undergone evolutionary changes in line with the dynamics of societal development. One of the propaganda theories used in relation to communication is Harold Dwight Laswel's theory.

Harold D Lasswell's Propaganda Theory. This theory adapts the theory of Freudianism, namely where this theory was born from the concept of dividing human personality into three elements which can be engineered through propaganda. The three elements are ego (ratio), internal desire (ID, personal pleasure), and superego (deepest feelings of conscience). The propaganda mechanism used is to convince the ego, then persuade the ID, to weaken the superego. This kind of propaganda is widely practiced in all locations from local to international levels, for example in multilevel marketing or social gatherings or profit sharing. And behaviorism theory, namely, this theory is a propaganda theory which assumes that social communities have a response to certain stimuli so that propaganda can influence the cognitive aspects of their life behavior. The peak of its implementation is to achieve the effect of mass support. According to Lasswell, propaganda is "an attempt to completely control opinion by using certain symbols, or speaking more concretely (although less accurately) through stories, rumors,

reports, photographs, and other forms of social communication. Propaganda has four goals: mobilizing one's own forces, strengthening friendships with fellow allies, influencing neutral parties, and overcoming the enemy's mentality." Lasswell is also famous for his leading communication model, namely who says what to whom in which channel with what effect.

Over time, propaganda again experienced a shift in meaning, namely, the dissemination of material and information for a specific purpose or mission. There are important principles in identifying propaganda, such as efforts to change public views. Changing views is carried out by influencing the emotional aspects of individuals en masse. The aim of propaganda is to establish similarities in beliefs, behavior and habits of the masses who are the targets of propaganda. It seems here that propaganda is mass communication. Mass communication is, "the dissemination of information carried out by a certain social group to listeners or audiences who are heterogeneous and spread everywhere.

One of the crimes categorized as transnational organized crime by the UN is Active Terrorist. The detailed definition of transnational organized crime is written in UN regulations (UNTOC) which combine two articles, namely Article 2 paragraph 1 (a) and Article 3 paragraph 2, consisting of:

a. Organized group

Organized group of criminals means a group consisting of three or more people, formed over a period of time and acting in an integrated manner with the aim of committing one or more serious criminal acts or offenses stipulated in accordance with this Convention, to gain directly or indirectly financial or other material benefits.

b. Characteristic transnational

Conducted in more than one State, carried out in one State but a significant part of the preparatory, planning, directing or control activities occurred in another State, carried out in one State but involving an organized criminal group involved in criminal activities in more than one State, carried out in one country but the main effect in another country.

Indonesia has ratified Transnational Organized Crime into Law no. 5 of 2009 concerning Ratification of the United Nations Convention Against Transnational Organized Crime (United Nations Convention Against Transnational Organized Crime). In article 3 paragraph (2) a criminal act is transnational in nature if: (a) it is committed in more than one country; (b) is carried out in one State but a significant part of the preparation, planning, direction or control activities occurs in another State; (c) is committed in one State but involves an organized criminal group engaged in criminal activities in more than one State; or (d) is committed in one State but has primary effects in another State.

2. Internet For Terrorist Purposes

Regarding the scope of internet use for terrorist purposes, Conway made a comparative classification of forms of internet use for terrorist purposes, which comes from expert opinion, including:

a. According to Furnell and Warren, namely: propaganda and publication; funding; dissemination of information; and secure communications.

b. According to Cohen, namely: planning; funding; operations and coordination; political action; and propaganda.

c. According to Thomas, namely: profiling; propaganda; anonymous or confidential communications; creating an atmosphere of fear through cyberspace; funding; command and control; recruitment and deployment of members; information gathering; minimize risk; data theft or manipulation; and attacks using incorrect information (misinformation).

According to UNODC, one of the purposes of internet use by terrorist organizations is propaganda. According to The World Book Encyclopedia, propaganda is a method used to influence people to believe in certain ideas (2000). Propaganda can take the form of campaigns of violence, rhetoric, recruitment, radicalization and incitement to terror. This can be seen in the form of multi-media communication that spreads ideology, explanations of the basis for justifying or promoting terrorist activities and orders to carry out war. Messages on the internet are available in the format of presentations, e-magazines, treatises, audio and video files, such as lectures and songs with religious or nasyid nuances, and video games created by terrorist organizations or their sympathizers.

Crime continues to grow along with the development of human civilization, with complex quality and quantity and variations in modus operandi. JE Sahetapy has stated in his writings that crime is closely related to and even part of the cultural output itself. This means that the higher the level of culture and the more modern a nation, the more modern crime will be in its form, nature and method of implementation.

With the current development of technology and information, the development of crime has shifted from being conventional to crimes that use the internet as a means of committing crimes. One of the crimes using the internet is the crime of terrorism, which uses propaganda and the spread of terrorist ideology using internet media carried out by terrorists. The crimes committed by terrorists are categorized as Cyber terrorism, where terrorist crimes are included in Transnational Organized

Crime.

Types of Cyber Terrorism Media

Global terrorism uses various types of new media in several ways to generate publicity and attract public attention. The diversity of media used is adjusted to the target audience they want to communicate with. An Al-Qaeda figure who is very active in using Internet applications in his terrorist activities is Al-Awlaki, who was born in New Mexico and received his degrees from the University of Colorado and the University of San Diego. The most obvious uses of Internet media that are used openly and can be accessed freely by all citizens of the world are websites, YouTube, social media and online magazines. In addition, online games are thought by intelligence officials to be a medium for them to coordinate in developing strategies. Terrorists use various online media applications optimally for their activities.

1. YouTube

YouTube has become one of the most effective parts of online media because apart from being able to reach the wider public, YouTube is also able to convey their messages audio-visually without being manipulated by mass media. Terrorist groups often use YouTube to report on their activities. If you can browse, lots of terrorism videos appear. Like the latest news that the Al-Qaeda group uploaded a video on YouTube showing Al-Qaeda holding a large meeting in Yemen recently. Analysts are examining the white car in the video, which is leading the convoy. The video initially appeared on several jihad sites and was then uploaded to YouTube. The faces of several Al-Qaeda members in the video are blurred. This shows concern that there is a new attack plan. The reason Al-Qaeda released the video, according to Bergen, the American national security analyst, speculated that the group did it for propaganda purposes, to show that they were still operating even though Osama Bin Laden was dead.

2. Website

Website posted by various terrorist groups with specific objectives. Some such as jehad.net and aloswa.org were created by Al-Qaeda supporters to show support for Osama Bin Laden, while others such as 7hj.7hj.com teach the use of hacking to serve Islamic organizations. However, currently these three sites cannot be accessed again. Meanwhile, Hezbollah is known to have operated three sites since February 1998: hizbollah.org is used as a central media office, moqawama.org describes its attacks against Israel, and almanar.com.lb provides news and information. These sites function to publish their history, mission, ideology, and overall goals in destroying their enemies. Plus, the website is used as a fundraising site in the hope of collecting funds from individuals and governments who are sympathetic to their actions. Donations are accepted online using "Pay Pal". Abu Musab al-Zarqawi's Al-Qaeda in Iraq was quite clever in their use of websites which they used to post video footage of them bombing, mutilating, and kidnapping their victims.

3. Online Games

Online Games, an increasingly popular way of disguising harmless messages for terrorists communicating online as “gamers” in online games. Many online forums are encrypted and require a password to join. Some may be infiltrated by government intelligence agents posing as online militants to find out about the terrorists' actions. They expanded the use of their media to have a wider reach or more effective communication between their members, to the point that the NSA and the British government massively infiltrated online multi-player role-playing games (MMORPG) such as World of Warcraft and Second Life to spy on them. - spy on communications between the terrorists. This fact was revealed by former NSA member, Edward Snowden, who gave secret documents to the British magazines The Guardian and the New York Times. In fact, these military actions are protected by law. If it is not balanced with strong analytical skills in game play to follow terrorist movements, then they will only carry out mass surveillance.

*Online game Second Life*used to spy on money laundering by these terrorists without banks they can obtain funds. According to Jeff Hermes, Legal Director of the Digital Media Project and the Berkman Online Media Law Network at the Harvard Center for Internet and Society, they revealed that they were trying to sell the money they earned from playing the games. Meanwhile, the online game World of Warcraft is used as a medium to discuss attack strategies. With these online games, they can manipulate the government and intelligence parties with fake identities. American intelligence wants to know about their latest terrorist action plans. After this secret became known, world IT companies such as Microsoft, Google, Facebook, Yahoo, Apple, Twitter and LinkedIn made public statements asking world governments to stop online surveillance. According to them, the government's spying actions disturb the privacy of game consumers and their comfort in playing online games.

Additionally, it was discovered by The Sun terrorists were using online games such as Call of Duty to plot and discuss subsequent attacks in private. Online games allow players to log in to a group to attack and discuss each other. They usually join an online gaming group and discuss the plot of the terror act they will carry out. There are various styles and missions in these games, from planting bombs to fighting one on one.

4. Social Media

Terrorists try to use various types of social media including Twitter and Facebook. Based on the latest research, international terrorist groups that challenge Western countries, such as Al-Qaeda, Hamas, and Hezbollah take turns recruiting through social networks such as Facebook and Twitter to attract various groups and gather intelligence. Currently, according to Gabriel Weimann from the University of Haifa, almost 90% of terrorist organizations use the Internet via social media. By using this tool, organizations can actively carry out recruitment without geographical limitations. Social media allows them to take the initiative to make requests to become "friends", upload videos, and they no longer use passive tools like websites. This is because websites tend to be one-way compared to social media which is interactive or based on Web 2.0 or even Web 3.0 because it is included in their ideology. Facebook and Twitter are used as forums for them to communicate between their members, recruit, and we can even see their instructions for making bombs.

In March 2013, Al Qaeda in the Islamic Magreb (AQIM) launched a Twitter account that gained more than 5,500 followers, and the AQIM account followed seven people including the official Somali terrorist group Al Shabaab and al Nusra in Syria, which in turn followed other rebel groups in Aleppo. Jean Paul Rouiller from the Geneva Center for the Training and Analysis of Terrorism said that social media is a vital medium for modern terrorist organizations. British intelligence agencies such as MI5, and their spy organizations GCHQ and MI6 always monitor various social media accounts including Facebook and Twitter which are suspected of being accounts belonging to terrorist groups. They exchange information and tactics through their social media accounts.

Apart from recruitment, according to Weimann, Facebook is used to collect information about military and political intelligence. Sometimes many people do not care about the identity of someone they accept as a social media friend and terrorists can use fake profiles to approach potential groups or individuals to support their actions and increase their strength in skills and knowledge relevant to their goals. For example, Weimann said that there were statements from Lebanon that Hezbollah was looking for material about Israeli military activities on Facebook. Countries such as the United States, Canada, England have instructed their military members to delete their personal information on Facebook otherwise Al-Qaeda will monitor them.

5. Online Magazine

Apart from these four media, they also have Sawt al-Jihad (Voice of Jihad), an online magazine that first appeared in 2004 to promote the achievements of the mujahideen. The website address of this magazine is http://www.sawtaljihad.org/ and is managed by the Al-Qaeda Committee in Saudi Arabia in English. It contains various issues related to their jihad actions, ranging from written posts to "Islamic Video" and "Jihad Video" links. However, when accessed now, the appearance of the site is no longer like an online magazine as seen below. Even if the link provided is accessed, such as "Islamic Jihad", it does not include content related to jihad, but leads to content outside the context of Islam and Jihad.

However, the existence of this online magazine proves that Al-Qaeda is a terrorist group that has various online media to communicate its community to the world. They try to spread their ideology from all directions and all media segments. These various terrorist methods through the use of various Internet media encourage readers or users to be more concerned about cybersecurity.

Cyber Terrorism Cases

There are several cases that are categorized as cyber-terrorism.

1. In 1988, the terrorist organization Guerrilla, within two weeks sent the Sri Lankan Embassy 800 emails per day. in the email sent it was called "we are the Internet Black Tiger and we are doing this to disrupt your communications." The Intelligence Department called this attack a terrorist attack on government computer systems.
2. October 2007, hackers attacked the website of Ukrainian President Viktor Jushenko.
3. The CIA published in January 2008 that hackers had succeeded in stopping power supply networks in several cities in the United States.

Meanwhile, many cases of cyber terrorism have occurred in various countries, including Indonesia. These cases include: (1) Sri Lankan embassies in various countries were flooded with nearly 800 emails, all containing threats (1997). The menacing group called themselves the Black Tigers; (2) a group of Chinese hackers shut down a Chinese satellite (1997); (3) internet sabotage occurred at the Babha Atomic Research Center, India (1998); (4) the information infrastructure in Estonia was attacked by a movement calling itself the Eurasian Youth Movement (2007); (5) cyber terrorism also occurred in Europe, carried out by Greek Security and Intrude. attacks were carried out against the computer systems of the European Organization for Nuclear Research (the world's largest nuclear development as of 2008); and (6) In 2016, the WannaCry ransomware virus attack appeared on several hospitals in almost 100 countries throughout the world, including Indonesia. The emergence of the virus is thought to be the result of an attack that used the internet to paralyze computer systems and hospital technology equipment.

This cyber terrorism movement is very dangerous and deserves to be watched out for, especially since the group running it is a terrorist group. For example, the perpetrator of the Bali Bombing (Imam Samudra) stated that the internet was the best tool to achieve his mission. He outlined this statement in his book entitled "I Fight Terrorists". He advised his juniors to learn the internet, so they are skilled like hackers. For them, the main goal is to share knowledge about hacking, as well as as a tool of political resistance.

4. DISCUSSION

The Nature and Meaning of Terrorism Crimes

Terrorism is an act of violence designed to cause fear with the aim of achieving political, ideological, or religious goals. In the context of Indonesian law, the definition of terrorism is regulated by Law Number 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism. According to this law, terrorism is defined as an act that uses violence or threats of violence that causes an atmosphere of terror or widespread fear among society. This definition emphasizes elements of violence and threats as the main tools used by terrorists to achieve their goals.

Historically, terrorism has existed in various forms throughout history, but modernization and globalization have changed the way terrorism is carried out and spread. In the modern era, terrorist groups use a variety of methods including bombings, hijackings, assassinations, and kidnappings to create fear and achieve their goals. Terrorism not only targets specific individuals or groups, but also often targets critical infrastructure and public places to maximize its psychological and political impact.

The meaning of terrorism also includes an ideological aspect where acts of violence are carried out to promote or enforce a certain ideology. This can be a political ideology, as seen in separatist groups, or a religious ideology, as espoused by extremist groups. Ideological terrorism often involves attempts to change the existing political or social order through violence and intimidation. Thus, acts of terrorism are often planned and executed with great care to ensure that the message the perpetrator of terrorism wishes to convey is clearly received by society and the government.

State Responsibility in the Perspective of International and National Law

From an international legal perspective, state responsibilities regarding terrorism are regulated in various conventions and frameworks coordinated by the United Nations (UN). One important convention is the 1999 International Convention for the Suppression of the Financing of Terrorism, which stipulates the obligations of states to prevent and punish acts of financing terrorism. This convention emphasizes that states must take the necessary steps to identify, freeze and confiscate funds used for terrorist purposes.

Apart from that, international law also underlines the importance of cooperation between countries in dealing with terrorism. International cooperation is necessary because of the cross-border nature of terrorism, which requires effective coordination between various jurisdictions to prevent and prosecute perpetrators of terrorism. The UN through various Security Council resolutions, such as Resolution 1373, emphasizes that member countries must cooperate in exchanging information, training and technical assistance to strengthen national capacity in fighting terrorism.

In the national context, Law Number 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism in Indonesia stipulates the state's responsibility to provide medical assistance, psychosocial rehabilitation and compensation to victims of terrorism. States have an obligation to ensure that victims of terrorism receive the care necessary to recover from the physical and psychological injuries they have experienced. Apart from that, the state is also responsible for providing financial compensation to victims as a form of reparation for the losses they have suffered.

National law also regulates preventive measures that countries must take to reduce the risk of terrorism. This includes strengthening intelligence, increasing security in strategic locations, and educating the public about the dangers of terrorism. States must ensure that law enforcement and security forces have the capabilities and resources necessary to detect and effectively act on terrorist threats.

The Concept of State Responsibility for Cyber Terrorism Through New Media

Cyber terrorism is a form of terrorism that is increasingly developing along with advances in information and communication technology. Cyber terrorism utilizes digital technology to launch terrorist attacks that can cause significant physical, economic or psychological damage. Examples of cyber terrorism attacks include hacking critical infrastructure such as power grids, banking systems, or communications networks.

States have a responsibility to improve cyber capabilities in detecting and preventing cyber terrorism attacks. This includes developing a strong cybersecurity infrastructure, training for experts in the field of cybersecurity, and increasing international cooperation to share information and technology. Countries also need to develop policies and regulations that regulate the use of information technology to ensure that technology is not misused by irresponsible parties.

A comprehensive legal framework is needed to deal with cyber terrorism. This includes regulations on data protection, network security, and sanctions against perpetrators of cyber terrorism. The law must be adaptive to technological

developments and able to cope with new threats that may emerge. The state must also ensure that law enforcement officials have the necessary tools and authority to take action against perpetrators of cyber terrorism.

Apart from that, the state is also responsible for providing protection and assistance to victims of cyber terrorism. This can take the form of technical assistance to restore systems affected by an attack, as well as medical and psychosocial assistance for individuals affected by the attack. Countries must ensure that victims of cyber terrorism have access to the resources they need to recover from such attacks.

The importance of international cooperation in confronting cyber terrorism cannot be ignored. Given the cross-border nature of cyber terrorism, cooperation between countries is essential to ensure that perpetrators cannot easily escape the law by hiding in other countries. The exchange of information and technology between countries can help in detecting and preventing attacks before they occur.

The state's overall responsibility in dealing with transnational terrorism and cyber terrorism includes prevention, action and recovery. Countries must be proactive in identifying and addressing the factors that allow terrorism to develop, including radicalization and terrorist financing. Enforcement efforts must be carried out in accordance with national and international law, respecting human rights and the principles of justice. Recovery for victims must be a priority to ensure that they get the support they need to return to normal life.

In facing increasingly complex challenges from terrorism and cyber terrorism, countries must continue to adapt and update their policies and strategies. The development of new technologies and changes in the modus operandi of terrorism require flexible and innovative responses. In doing so, countries can ensure that they are able to protect their citizens and contribute to global security.

This research emphasizes the importance of state responsibility in facing the threat of transnational terrorism and cyber terrorism. Through strengthening legal frameworks, increasing cyber capacity, and international cooperation, countries can more effectively address these threats and ensure better protection for their citizens. Only with a comprehensive and coordinated approach can countries reduce the risk of terrorism and create a safe and peaceful environment for all.

5. CONCLUSION

This research confirms that terrorism, both in traditional forms and in more sophisticated forms such as cyber terrorism, is a serious threat that requires a strong and effective legal response from the state. Based on the analysis that has been carried out, it can be concluded that the nature and meaning of criminal acts of terrorism in national and international law shows that terrorism is an act of violence that aims to cause fear in society in order to achieve political, ideological or religious goals. These definitions and characteristics are consistent across various national laws and international conventions.

In the context of state responsibility, this research finds that the state has significant legal and moral obligations in preventing, handling, and providing protection and reparations for victims of criminal acts of transnational terrorism. This responsibility is regulated by various international conventions such as the International Convention for the Suppression of Terrorist Bombings (1998) and the International Convention for the Suppression of the Financing of Terrorism (1999), as well as national laws and regulations such as Law Number 15 of 2003 concerning Eradication of Criminal Acts of Terrorism.

Research also shows that information and communication technology has changed the way terrorism is carried out, introducing a new phenomenon known as cyber terrorism. Countries must increase their cyber capacity to detect and prevent these attacks. Analysis of various cases of cyberterrorism in various countries shows that this threat requires a comprehensive and dynamic legal framework that is able to respond to changes in technology and terrorist modus operandi.

The concept of state responsibility towards citizens involved in criminal acts of transnational terrorism, especially in the form of cyber terrorism, emphasizes the need for the state to not only focus on aspects of prevention and prosecution, but also on efforts to protect and rehabilitate victims. This includes the provision of medical assistance, psychosocial rehabilitation and adequate compensation for victims, as provided for in national law and supported by international conventions.

Overall, this research emphasizes the importance of international coordination and cooperation in dealing with criminal acts of transnational terrorism and cyber-terrorism. Countries need to adopt best practices from various jurisdictions and continually update their legal frameworks to meet evolving threats. It is hoped that the results of this research can provide a significant contribution to the development of effective policies and laws in dealing with the threat of transnational terrorism and cyberterrorism, as well as increasing protection for citizens from increasingly complex and dynamic terrorist attacks.

REFERENCES

[1] Adji, I. S. (2017). Terorisme dan HAM dalam Terorisme: Tragedi Umat Manusia. *Jakarta: OC Kaligis & Associates*.

[2] Al Qurtuby, S. (2022). Terrorism in Indonesia. In *Terrorism and Counter-terrorism in Saudi Arabia and*

Indonesia (pp. 189–243). Springer.

[3] Ampriyanto, F. M., & others. (2018). POLITIK HUKUM PERUBAHAN UNDANG-UNDANG NOMOR 15 TAHUN 2003 TENTANG PEMBERANTASAN TINDAK PIDANA TERORISME (Studi Analisis Bab Penanggulangan).

[4] Chandler, M., & Gunaratna, R. (2007). *Countering terrorism: can we meet the threat of global violence?* Reaktion Books.

[5] Denning, D. E. (2000). Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives. *Focus on Terrorism*, *9*(1), 71–76.

[6] Fraser, N. (2020). Transnationalizing the public sphere: On the legitimacy and efficacy of public opinion in a post-Westphalian world. In *Habermas and Law* (pp. 379–402). Routledge.

[7] Kelsen, H. (2019). *Teori Hukum Murni: Dasar-Dasar Ilmu Hukum Normatif*. Nusamedia.

[8] Komalasari, N. (2011). Pidana Mati Dalam Sistem Hukum Indonesia (Studi Tentang Efektivitas Sanksi Pidana Mati Dalam Peraturan Perundang Undangan No. 1 Tahun 2002 Jo Undang-Undang No. 15 Tahun 2003 Tentang Erorisme dan Undang-Undang No. 35 Tahun 2009 Tentang Narkotika).

[9] Kronstadt, K. A., & Vaughn, B. (2004). CRS Report for Congress. In *Foreign Affairs, Defence and Trade Division United States of America: Congressional Research Services, The Library of Congress. http://www. au. af. mil/au/awc/awcgate/crs/rs22009. pdf (accessed 24 March 2010)*.

[10] Kurtulus, E. N. (2017). Terrorism and fear: do terrorists really want to scare? *Critical Studies on Terrorism*, *10*(3), 501–522.

[11] Kuru, H. (2023). Cyber Terror Threats Against Nuclear Power Plants. *Journal of Learning and Teaching in Digital Age*, *8*(2), 237–244.

[12] McQuail, D. (2010). The future of communication studies: A contribution to the debate. *Media and Communication Studies Interventions and Intersections*, *27*.

[13] Muhlashin, I. (2021). Negara Hukum, Demokrasi Dan Penegakan Hukum Di Indonesia. *Jurnal Al-Qadau: Peradilan Dan Hukum Keluarga Islam*, *8*(1), 87–100.

[14] Raj, P., & Yadav, S. (2022). Cyber Terrorism: A Threat to Cyber World. *Emerging Trends in Technology & Its Impact on Law*, *1*.

[15] Ridwan, M., Suhar, A. M., Ulum, B., & Muhammad, F. (2021). Pentingnya penerapan literature review pada penelitian ilmiah. *Jurnal Masohi*, *2*(1), 42–51.

[16] Saputra, R., Sinaulan, R. L., & Farhana, F. (2023). Peranan Detasemen Khusus 88 Anti-Teror Dalam Penanganan Tindak Pidana Terorisme Dalam Perspektif Hak Asasi Manusia. *Jurnal Multidisiplin Indonesia*, *2*(9), 2764–2786.

[17] Satino, S., Yuli, Y., Surahmad, S., & Andriyanto, A. (2023). Diversi Sebagai Salah Satu Bentuk Usaha Dalam Menyelesaikan Perkara Pidana Terhadap Anak Melalui Restorative Justice. *IKRA-ITH HUMANIORA: Jurnal Sosial Dan Humaniora*, *7*(3), 329–339.

[18] Saul, B., & Heath, K. (2021). Cyber terrorism and use of the internet for terrorist purposes. In *Research Handbook on International Law and Cyberspace* (pp. 205–230). Edward Elgar Publishing.

[19] Schmid, A. P. (2011). The definition of terrorism. In *The Routledge handbook of terrorism research* (pp. 39–157). Routledge.

[20] Shidarta, S. (2020). Bernard Arief Sidharta: Dari Pengembanan Hukum Teoretis ke Pembentukan Ilmu Hukum Nasional Indonesia. *Undang: Jurnal Hukum*, *3*(2), 441–476.

[21] Suharto, Y. (2020). PENDIDIKAN ISLAM RAHMATAN LIL ALAMIN; MENOLAK TERORISME. *Jurnal Pendidikan Islam*, *10*(1), 61–73.

[22] Syihab, M. A., & Hatta, M. (2023). Metode Penanggulangan Tindak Pidana Terorisme Di Indonesia. *Cendekia: Jurnal Hukum, Sosial Dan Humaniora*, *1*(1), 13–27.

[23] Vita Indah, P. (2021). *Kebijakan Politik Luar Negeri Indonesia terhadap Pengungsi Asing dan Pencari Suaka Pada Era Reformasi Perspektif Siy{\=a}sah Dauliyah*. IAIN PURWOKERTO.

[24] Wahjono, P., & Syamsuddin, N. (2009). Pengantar Ilmu Politik. *PT Raja Grafindo Persada, Jakarta*.

[25] Yuliana, R., & Hasibuan, Z. A. (2022). Best practice framework for information technology security governance in Indonesian government. *International Journal of Electrical and Computer Engineering*, *12*(6), 6522.