International Journal of Law Analytics (IJLA)
Vol. 3, No. 4, (November) 2025: 331-348

Criminological Aspects Related to Terrorism Strategy and Propaganda via the Internet (Case Study of Cyber-Terrorism in Indonesia)

Antonius Maria Laot Kian[1]*, Slamet Sarwo Eddy[2], Syntia Wati[3]
[1,2]Magister Hukum Universitas Proklamasi 45 Yogyakarta, [3]Fakultas Hukum Universitas Proklamasi 45 Yogyakarta
Corresponding Author: Antonius Maria Laot Kian
antoniusmarialaotkian2020@gmail.com

A R T I C L E I N F O

Keywords: Criminology, Terrorism Strategy, Internet, Cyber-Terrorism

Received: 7, October
Revised: 27, October
Accepted: 28, November

A B S T R A C T

This article analyzes criminological aspects of Internet-based terrorism strategy and propaganda, with a case study on cyber-terrorism in Indonesia. While terrorism has existed since 1949, sophisticated technology has accelerated its dissemination, leading to the rapid growth of cyber-terrorism. Individuals exploit internet networks to spread propaganda, often targeting an unaware public. Criminology aids in understanding these crimes by identifying perpetrators' motivations and profiles, activity characteristics, and operational patterns. This phenomenon generates significant public concern. Consequently, this article aims to foster greater public awareness and provide essential knowledge on how to behave when confronted with online terrorist propaganda, promoting a more vigilant and informed society.

DOI: https://doi.org/10.59890/ijla.v3i4.89
E-ISSN: 3032-4041
https://slamultitechpublisher.com/index.php/ijla/index

INTRODUCTION

Terrorism as a movement is certainly very worrying because the teachings or information disseminated often clash and conflict with religious values, morality and culture in society (Rumadan & Ridwan, 2020). Interestingly, the perpetrator of this terrorism consciously knows that his actions will certainly not be successful against the state security apparatus, but that is not what he wants, but rather the effects of terror that will arise and the emergence of a growing sense of fear in society, with the hope that there will be instability in social conditions. and politics in Indonesia (Rumadan & Ridwan, 2020). This can be seen from several acts of terrorists who carried out suicide bombings (Respati et al., 2020), shooting of guard posts (Martin & Pasaribu, 2022), and killing ordinary people for no good reason (Online Legal Team, 2023). These actions cause conditions in people's lives to become uncomfortable, restless, and peace is reduced.

Terrorism is actually nothing new in Indonesia. Sulastiana stated that terrorism trends in Indonesia are classified into 4 (four) periods. These periods can be described as follows:

1) The First Period, was the DI/TII era from 1949 to 1954 which wanted to form the Islamic State of Indonesia. This movement was led by Kahar Muzakar in Sulawesi, Kartosuwiryo in West Java, and Daud Bireuh in Aceh.
2) The second period was the Jemaah Islamiyyah period which began in 1983, led by Abdullah Sungkar and Abu Bakar Baasyir. This terrorist group started from the Al Mukmin Islamic Boarding School in Sukoharjo and spread its radical beliefs from this Islamic boarding school. Jemaah Islamiyyah existed in Indonesia until the early 2000s and succeeded in carrying out the Bali Bombing 1, Bali Bombing 2, the Australian Embassy Bombing, and the JW Marriot Bombing.
3) Third Period, is ISIS. These terrorists are influenced by the global terrorism movement centered in Iran and Syria.
4) The Fourth Period, is a period of technological development that makes communication network trends, ideological dissemination and recruitment different. ISIS used blogs, websites, social media and instant messengers to spread its ideology, communicate or even recruit new members (Admin, 2018).

The trend of terrorism in the fourth period is currently a serious concern for the Government. In the midst of the euphoria of technological development in society, of course there are many challenges that must be faced, especially for people who have not been able to filter out negative things from the sophistication of technology that has become grounded. As is known, in this era of technological development, information technology in the field of computers and internet networks is developing very rapidly. The internet, which is one of the results of information technology, is an information resource that can reach the entire world (Mildawati, 2000). Advances in internet networks make the communication process easier.

Digital communication media is one of the most obvious changes that can be felt by the general public (Nurdina, 2024). With digital communication media,

massive dissemination of information can be carried out by the public. The ease of disseminating information has had a positive impact on society, but there are also quite a few negative impacts that are detrimental and must be felt as the impact of current technological developments, one of which is the phenomenon of propaganda for terrorism via the internet, which is currently known as cyber-terrorism. Bambang and Fitriana explained that cyber-terrorism is an activity and/or method used by a number of terrorist networks or groupss (A.S. & Fitriana, 2017).

Terrorists use the internet to spread ideology and recruit new members. Platforms such as social media, online forums, and anonymous websites also allow terrorist perpetrators to convey their messages easily and quickly without geographical boundaries. Propoganda is an effort made by a group of people or an organization to influence people. The term propaganda may have painted a negative or bad image in someone's mind (Munthe, 2012). Internet propaganda has a special appeal, especially for the younger generation who are often the main targets of terrorists. In such a context, the digital literacy of Indonesian society becomes an important issue because many are not yet able to recognize or realize the threats hidden in online content.

Criminology is a field of science that studies crime (Edrisy, 2023) become an important tool in understanding the phenomenon of cyber-terrorism. The criminological aspect allows the public to understand the motivations, patterns of action and strategies used by terrorist perpetrators via the internet. An approach through the field of criminology also helps in identifying the characteristics of digital propaganda, ranging from the content distributed to techniques for manipulating public opinion carried out by terrorist groups. In many cases, this propaganda not only creates fear, but also aims to mobilize sympathizers to take real action. Therefore, understanding aspects of criminology is important for developing effective prevention and response strategies.

The importance of this article is as a medium for educating people who do not yet have the ability to recognize digital propaganda which is feared that people will easily be exposed to radical messages. Traditional approaches to dealing with terrorism are often not relevant enough in the digital era, where perpetrators can operate anonymously and attacks are not always physical. By understanding aspects of criminology, such as motivations, propaganda techniques, and cybercrime networks, we can develop more adaptive strategies to combat this threat.

THEORETICAL REVIEW

The Concept of Criminology

Etymologically, criminology comes from the words crimen which means crime and logos which means science or knowledge, so that criminology is a science or knowledge that studies crime (Susanto, 2011). The term criminology was previously called criminal anthropology (A.S., 2010) [30], which means that criminology is a process of law formation, law violation, and reactions to law violations. Thus, in fact criminology does not only study crime but also includes

the process of forming laws, breaking the law, and the reactions given to perpetrators of crimes.

In relation to criminal acts of terrorism, criminology as a science that studies criminal behavior and the factors behind it provides a systematic approach to analyzing how terrorist groups use the internet as a strategic medium. The theory that can be used as a reference for analysis in this case is Sociogenic Theory. This theory explains that the cause of purely sociological or social psychological evil behavior is the influence of deviative social structures, group pressure, social roles, social status, or wrong symbolic internalization. Evil behavior is formed by a bad and evil environment, unattractive school conditions and relationships that are not guided by moral and religious values (Susanti & Rahardjo, 2018). This theory reveals that the causes of crime are influenced by surrounding environmental factors, including family, economic, social, cultural, defense and security and technological discoveries (Lutfi et al., 2022).

The Sociogenic Theory

According to Sociogenic Theory in criminology, crime patterns committed by terrorists are influenced by social and environmental factors that shape individual or group behavior. This theory emphasizes that criminal acts, including terrorism, do not arise spontaneously, but rather are the result of a social interaction process that influences the perpetrator's thought patterns, values and behavior. In criminal acts of terrorism, individuals often come from environments that experience social, economic or political pressure, so that in the end a feeling of dissatisfaction or feeling of being alienated emerges.

The pattern of terrorist crimes emerges when someone interacts with a group that has an extremist ideology, where radical values are instilled through propaganda, indoctrination, or intense social relationships. Radical means that the values brought about in criminal acts of terrorism make people think at their roots (Sugiono, 2017), namely thinking down to the essence, essence or down to the substance of what is thought.

METHODOLOGY

This research is a type of empirical normative legal research. Empirical normative legal research is legal research that examines the factual implementation or implementation of positive legal provisions (legislation) and contracts on each specific legal event that occurs in society in order to achieve predetermined goals (Muhaimin, 2020). As previously mentioned, this research will analyze how aspects of criminology work to understand the strategy and propaganda of terrorism via the Internet, with a case study on cyber-theorism in Indonesia. Through this type of empirical normative legal research, the author identifies the legal framework related to cyber-terrorism in Indonesia, such as Law Number 5 of 2018 concerning Eradication of Criminal Acts of Terrorism and the Information and Electronic Transactions Law (UU ITE), which then analyzes the implementation of these laws in dealing with propaganda and terrorism strategies via the internet. The connection with this research is to see the extent

to which the rule of law has been implemented effectively in dealing with cyber-terrorism, as well as identifying challenges or gaps in its implementation.

Furthermore, the research approaches used in this research are conceptual approaches, legislation, legal history, and case approaches (Muhaimin, 2020). Meanwhile, the types of data used are secondary data and primary data. A conceptual approach is carried out by analyzing basic concepts regarding cyber-terrorism, digital propaganda strategies, and criminological aspects. This helps understand the motivations, action patterns and impact of digital propaganda. Next, a legislative approach is taken by examining how the laws regulate cybercrime and terrorism, including how these regulations are interpreted and implemented in Indonesia. Next, through a legal history approach, tracing how terrorism began and tracing the development of regulations and policies regarding terrorism in Indonesia, from conventional terrorism to internet-based crimes. Finally, regarding the case approach, in this research the author also describes examples of cyber-terrorism cases in Indonesia so that we can find out how propaganda in the real world is carried out by terrorist perpetrators.

Secondary data sources were obtained through literature study and document study. Literature study includes; books, journals, seminar proceedings, papers, legal dictionaries, legal encolepdia, legal literature dictionaries or other written legal materials. In addition to literature studies, document studies also include; hierarchical or tiered legal documents, legal regulations, jurisprudence, agreements/contracts and other documents. Meanwhile, primary data is data directly obtained from the community, subjects studied at institutions, or community groups, direct actors who can provide information to researchers known as respondents and informants (Muhaimin, 2020).

Data analysis in this legal research is carried out qualitatively, comprehensively and completely, resulting in more perfect normative-empirical legal research results. Qualitative analysis is data analysis that does not use numbers but rather provides verbal descriptions of the findings and therefore prioritizes the quality of the data, and not quantity. Through this research, we will analyze how propaganda strategies are carried out by terrorist groups on the internet, what the motivations and crime patterns of cyber-terrorism perpetrators are, and how society responds to this propaganda. This analysis allows a comprehensive understanding of cyber-terrorism, from the legal side to its impact on society.

RESEARCH RESULTS

History of Terrorism in Indonesia

Before understanding the history of terrorism in Indonesia, it is first necessary to understand how terrorism is defined. Ashie provides several definitions of terrorism, namely as follows:

1) Terrorism refers to the criminal tactics of conflict containment, involving some of the same acts of violence that would qualify as war crimes if a state of war existed - deliberate attacks on civilians, non-combatants and third

parties, deliberate killings, taking hostages and murder detainees (abducted people);
2) Terrorism is any attack, or threat of attack, against an unarmed target, intended to influence, change, or divert major political decisions;
3) It is generally defined as the deliberate use of violence and intimidation directed at a broad audience to force a society or its government to agree to politically or ideologically motivated demands;
4) The use of violence with the aim of creating fear in a wider audience to prevent parties from doing something, or, conversely, to force them to carry out a certain behavior;
5) Terrorism is the planned use or threat to use violence by individuals or subnational groups against noncombatants to achieve political or social objectives through intimidation of large audiences beyond those of the immediate victim (Ashie, 2015).

Furthermore, according to Jenkins, who is a legal expert from South America, defines terrorism as a classic form of criminal acts such as murder, arson, use of explosives, but differs from ordinary crimes in carrying out the intention, namely deliberately causing panic, chaos and terror in public (Jenkins, 1990). From these definitions, it can be concluded regarding terrorism that terrorism is the use of acts of violence or threats of violence that are deliberately designed to create fear, chaos or intimidation among the wider community, where these actions are usually directed at non-combatant targets, including civilians. with the aim of influencing, changing, or forcing the making of a political, social, or ideological decision by involving various forms of crime such as murder, hostage-taking, or the use of explosives executed to obtain a psychological impact that extends beyond the victim.

As previously explained, terrorism is actually nothing new in Indonesia, where the trend of terrorism in Indonesia is classified into 4 (four) periods, namely as follows:

1) The First Period, was the DI/TII era from 1949 to 1954 which wanted to form the Islamic State of Indonesia. This movement was led by Kahar Muzakar in Sulawesi, Kartosuwiryo in West Java, and Daud Bireuh in Aceh. At the beginning of independence, the Republic of Indonesia was facing various attacks, both physical and non-physical. The Dutch, who did not recognize Indonesia's independence, then carried out aggression to take over power. Of course, Kartosuwirjo did not remain silent. On August 14 1947, after the First Dutch Military Action, he officially declared war on the Netherlands. Taking advantage of this momentum, Kartosuwirjo considered the West Java area as an area that was de facto under his control. At that time, DI had not yet been officially established. He also first formed a military force called the Indonesian Islamic Army (TII) which was stationed in the mountainous areas around West Java (Garadian, 2024) [15].
2) The second period was the Jemaah Islamiyyah period which began in 1983, led by Abdullah Sungkar and Abu Bakar Baasyir. This terrorist group started from the Al Mukmin Islamic Boarding School in Sukoharjo and spread its radical beliefs from this Islamic boarding school. Jemaah Islamiyyah existed

in Indonesia until the early 2000s and succeeded in carrying out the Bali Bombing 1, Bali Bombing 2, the Australian Embassy Bombing and the JW Marriot Bombing. The 2003 Jakarta bombing (also called the 2003 JW Marriott bombing) was a bomb explosion at the JW Mariott hotel in the Mega Kuningan area, Jakarta, Indonesia at 12:45 and 12:55 WIB on Tuesday, 5 August 2003. The explosion came from a bomb suicide car using a car driven by Asmar Latin Sani. The explosion killed 12 people and injured 150 people (Wikipedia, 2024).

3) Third Period, is ISIS. These terrorists are influenced by the global terrorism movement centered in Iran and Syria. These terrorists are influenced by the global terrorism movement centered in Iran and Syria. Radicalism arises from various axes such as social, economic and political (Hutabarat & Larasati, 2023).
4) The Fourth Period, is a period of technological development that makes communication network trends, ideological dissemination and recruitment different. ISIS used blogs, websites, social media and instant messengers to spread its ideology, communicate or even recruit new members. The terrorists carried out their movements through social media and internet archives which they produced and then spread through social media (Rizki, 2024) [18].

From various trends or history of terrorist movements in Indonesia, this terrorist phenomenon is often based on religious understanding. Terrorist perpetrators often use religious narratives to justify their actions as well as attract sympathy from someone who feels marginalized socially, politically or economically. Such terrorists have certainly deviated very far from true religious teachings which emphasize peace and compassion. This abuse of religion creates a big challenge for the government and society in terms of distinguishing between true religious teachings and radical ideological concepts that are used to justify acts of terrorism.

Terrorism Regulations in Indonesia

The rule of law which is a term attached to Indonesia as mandated in Article 1 Paragraph (3) of the 1945 Constitution of the Republic of Indonesia which states that Indonesia is a state of law, has the consequence that the Indonesian state must provide legal protection to its citizens, namely the Indonesian people. Hadjon provides a definition of legal protection as a protection of honor and dignity, as well as recognition of human rights possessed by legal subjects based on legal provisions from arbitrariness or as a collection of regulations or rules that will be able to protect one thing from another (Hadjon, 1987). Meanwhile, Satjipto Rahardjo stated that legal protection is an effort to protect a person's interests by allocating a human right of power to him to act in the context of those interests (Rahardjo, 2003). From these definitions, it can be concluded that legal protection is a government effort through the dimensions of prevention, recognition of rights, and granting legal powers to individuals in order to guarantee justice and protect their rights.

The principles of legal protection in Indonesia have a strong foundation, namely Pancasila as the state ideology and philosophy based on the concepts of Rechstaat and Rule of Law (Martien, 2023). Through this concept, it is emphasized that legal protection of human dignity is based on the values of Pancasila, while legal protection of government actions originates from the recognition and protection of Human Rights. This concept, which originates from Western legal traditions, aims to establish limits and obligations for both society and government, thereby creating balance in the exercise of power.

In connection with this legal protection, terrorism in Indonesia is included in the criminal sanctions section. Criminal sanctions are the imposition of suffering on someone who is found guilty of committing a crime (criminal act) through a series of judicial processes by the power (law) specifically given for that matter, with the imposition of criminal sanctions it is hoped that the person will not commit another criminal act (Sari, 2022). By imposing criminal sanctions, it is hoped that people will no longer commit criminal acts.

In order to provide legal protection to the Indonesian people and as an effort to prevent the occurrence of criminal acts of terrorism in the various tragedies that have occurred, the Indonesian Government issued a Government Regulation in Lieu of Law of the Republic of Indonesia (Perpu) Number 1 of 2002 concerning the Eradication of Criminal Acts of Terrorism. In this Perpu, it is explained that terrorism has taken lives regardless of victims and has caused widespread public fear, or loss of independence, as well as loss of property, therefore it is necessary to take steps to eradicate it. Not only that, terrorism has a wide network so it is a threat to national and international peace and security. Therefore, given the urgent need, it is necessary to regulate the eradication of criminal acts of terrorism with a Government Regulation in Lieu of Law. The Perpu was then promulgated as law through the promulgation of Law of the Republic of Indonesia Number 15 of 2003 concerning the Stipulation of Government Regulations in Lieu of Law Number 1 of 2002 concerning the Eradication of Criminal Acts of Terrorism, Becoming Law. This law was enacted in order to restore orderly and safe social life and to provide a strong legal basis and legal certainty in overcoming urgent problems in eradicating criminal acts of terrorism. This is also considering that the Perpu itself has a time limit for its validity so it must be immediately stipulated through law.

It doesn't just stop at this Law, then in 2018 the regulations regarding criminal acts of terrorism were again changed through the Law of the Republic of Indonesia Number 5 of 2018 concerning Amendments to Law Number 15 of 2003 concerning the Determination of Government Regulations in Lieu of Laws. Number 1 of 2002 concerning Eradication of Criminal Acts of Terrorism, Becomes Law (hereinafter referred to as Law Number 5 of 2018). According to the Explanation to Law Number 5 of 2018, it is stated that in order to provide a stronger legal basis to guarantee legal protection and certainty in the prevention and eradication of criminal acts of terrorism, as well as to meet the legal needs and development of society, it is necessary to make changes proportionally and consistently. maintain a balance between the need for law enforcement, protection of human rights, and socio-political conditions in Indonesia. This

amendment to the Law provides a normative basis that the state is responsible for protecting victims in the form of medical assistance, psychosocial and psychological rehabilitation, and compensation for those who die and compensation. However, the state's responsibility in protecting victims does not eliminate the victim's right to receive restitution as compensation for losses caused by the perpetrator to the victim.

Several articles in Law Number 5 of 2018 contain criminal threats against perpetrators of terrorism, one of which is as stated in Article 12B Paragraph (3) and Paragraph (4), as follows:

> Paragraph (3)
> Every person who deliberately creates, collects and/or disseminates writings or documents, both electronic and non-electronic for use in training as intended in paragraph (1) shall be punished by imprisonment for a minimum of 3 (three) years and a maximum of 12 (twelve) years.) year.
> Paragraph (4)
> Every Indonesian citizen who is convicted of terrorism as intended in paragraph (1) to paragraph (3) may be subject to additional criminal penalties in the form of revocation of the right to have a passport and border crossing passes for a maximum period of 5 (five) years.

What is meant by terrorism in Article 1 Number (2) of Law Number 5 of 2018 is an act that uses violence or threats of violence that creates an atmosphere of terror or widespread fear, which can cause mass casualties, and/or cause damage. or destruction of vital strategic objects, the environment, public facilities, or international facilities with ideological, political or security disturbance motives. The threat of violence referred to is as regulated in Article 1 Number (4) of Law Number 5 of 2018, namely every unlawful act in the form of speech, writing, images, symbols or body movements, either with or without the use of means in the form of electronic or non-electronic which can cause fear of people or society at large or curb the essential freedoms of a person or society.

These two articles provide a strong legal basis for law enforcement officials to impose criminal penalties on perpetrators of terrorism not only for direct acts of terrorism but also as a form of invisible threat. This reflects awareness of changes in the pattern of terrorist crimes, which now increasingly utilize technology to spread fear. Law Number 5 of 2018 allows a more adaptive approach in dealing with modern threats, such as digital propaganda and cyber-terrorism, which can create terror effects without involving direct physical action.

Case Study Cyber-Terorisme di Indonesia

Below are some cases studies of cyber-terrorism in Indonesia. First, cyber-terrorism that occurred in Bali involving the perpetrator on death row in the 2002 Bali bombing case, Abdul Azis alias Imam Samudra. This crime was Ali's first crime that utilized cyberspace for the purposes of provocation and propaganda for terrorist networks. Due to this action, all parties are required to be alert to the emergence of similar cases which are very dangerous crimes (RH, 2006).

Second, hospitals became victims of cyber-terrorism attacks with the WannaCry ransomware attack spreading widely throughout the world, including Indonesia. The program even took hostage the computer systems of a number of hospitals, making it difficult to provide medical services to patients. This attack is used by hackers to infect the victim's computer automatically, without requiring human intervention and this ransomware will lock data and computer systems so that they cannot be accessed, after which the perpetrator demands a ransom of IDR 4,000,000.00 (four million rupiah) in the form of currency. Bitcoin virtual money so you can unlock the encryption key on your computer. However, even though the requested ransom has been sent, there is no guarantee that the perpetrator will actually send the encryption key (Yusuf, 2017). Attacks like this underscore the importance of strengthening cybersecurity infrastructure to prevent greater losses.

Third, the data hack that befell the Ministry of Communication and Informatics (Kominfo) is one of a series of cybercrime cases that emerged throughout 2022. The perpetrator of the attack, Bjorka, succeeded in accessing and stealing SIM card registration data managed by Kominfo. This incident occurred due to a security gap in the Kominfo server system. Most of Bjorka's hacking victims were domestic companies that had vulnerabilities in their server security systems (Admin, 2023). This incident not only tarnished the reputation of government institutions but also increased the risk of misuse of people's personal data by irresponsible parties.

From these three cases, it can be seen that cyber-terrorism in Indonesia is not only a threat to national security but also to vital sectors such as health and public data. These incidents emphasize the need for vigilance, strengthening regulations, increasing public awareness, and investing in cybersecurity infrastructure to provide protection for digital assets from increasingly complex attacks.

DISCUSSION

Criminological Aspects related to Terrorism Strategy and Propaganda via the Internet

Cyber-terrorism is a new form of crime with several specific conditions to be categorized as cyber-terrorism (Mumtaaz et al., 2021). Mac Donald identified cyber-terrorism as attacks on critical national infrastructure or acts of intimidation against civilians or government employees using the power of internet networks and computer technology (MacDonald, [24]. *Cyber-terrorism is also a modernized form of conventional terrorism* (Danastri, 2011), as an unlawful attack on computer networks, stored information networks to intimidate the government or its people resulting in violence against individuals, groups or Indonesian government property, thereby causing danger and fear.

The relationship between criminology and terrorism strategies and propaganda via the internet lies in criminology's ability to understand the patterns, motivations and impacts of these criminal acts. As explained earlier, the discussion of criminological aspects related to cyberterrorism is closely related to

Sociogenic Theory. Here are the main points of the theory applied to cyberterrorism:

1. Root Causes in Social, Economic, and Political Pressures: Potential terrorists often come from environments marked by injustice, oppression, marginalization, or a lack of opportunity. These pressures create a foundation of frustration and alienation. Concrete Example: A highly skilled but unemployed programmer living in a region with a repressive government and widespread censorship. His daily experience of political injustice and lack of economic future fuels a deep-seated anger and a sense of being an outsider in his own society.
2. The Role of Social Interaction and Group Dynamics: The individual's radicalization is not done in isolation. It occurs through interaction with a group (online or offline) that promotes an extremist ideology. The group provides a sense of belonging, purpose, and identity. Concrete Example: The frustrated programmer begins to frequent encrypted online forums where a hacktivist group operates. In these forums, he finds a community that shares and validates his grievances. He is no longer a lone, alienated individual but part of a "cause."
3. Indoctrination through Propaganda and Ideology: The group actively instills its radical values through a structured process. This can include propaganda (e.g., videos, manifestos), indoctrination (us vs. them narratives), and the glorification of "cyber jihad" as a legitimate and heroic response to oppression. Concrete Example: In the online forum, senior members share edited videos showing the "crimes" of their enemy, publish ideological texts framing cyberattacks as a moral duty, and provide technical guides for launching attacks. The programmer absorbs this worldview, which redefines his criminal activity as a righteous act.
4. The Emergence of Cyberterrorist Behavior: The final step is the translation of this newly formed identity and belief system into action. The individual, now fully integrated into the group's ideology, carries out cyberterrorism acts (e.g., hacking critical infrastructure, spreading disinformation, launching DDoS attacks on government sites) as a logical outcome of their social conditioning. Concrete Example: After months of interaction and indoctrination, the programmer uses his skills to deploy a ransomware attack on a government ministry's website, crippling its services. He does this not just as a technical exploit, but as a politically and ideologically motivated act of "war" against the system he now despises. In short, Sociogenic Theory shifts the focus from the individual as a "lone wolf" to the social environment and processes that manufacture a cyberterrorist. The crime is the final symptom of a deeper social disease.

Social media and the internet are often the main tools in the process of terrorist crimes which enable terrorist perpetrators to create digital subcultural communities that strengthen the collective identity of terrorist perpetrators. This pattern of crime also involves a rationalization process where the perpetrator of terrorism believes that his actions, even though they violate the law, are considered morally or ideologically justified because they are seen as a struggle

against injustice. Thus, through sociogenic theory, society can observe social interactions and environmental dynamics that influence crime patterns in acts of terrorism.

In relation to the motivation of terrorist perpetrators, it can be identified from ideological, political, social and psychological factors. The ideological factor is one of the main factors in the perpetrator's belief that his actions are a form of sacred struggle or a moral obligation to achieve certain goals, such as establishing a state based on religious law or fighting for groups that are considered oppressed. Another example is the suicide bombing, which was carried out by terrorists in the midst of a crowd, which is considered to be the cause of many immoral acts, so that terrorists carry out suicide bombings for the reason of evil for the good of humanity. Apart from that, political motivation also plays an important role, especially when the perpetrator feels that he does not have an official and legal channel to express dissatisfaction with government policies or certain political situations. Social factors such as marginalization, discrimination, or economic injustice can also trigger someone to join a terrorist group that offers a sense of identity, solidarity, and shared goals. Furthermore, psychological factors such as feelings of frustration or a desire for revenge, or the need for recognition are often personal motivations for the perpetrator.

In many cases, the propaganda and emotional manipulation carried out by terrorists over the internet reinforces these motivations, making individuals feel that acts of terror are the only way to achieve the change they desire. One common example is the use of social media to distribute videos, infographics or text messages that present narratives of the struggle of terrorists as something heroic and defending justice. Such perpetrators are usually terrorist groups such as the Islamic State of Iraq and Syria (ISI), which is a jihadist militant group that wants to establish an Islamic caliphate (Tysara, 2023) [34], for example, by utilizing platforms such as YouTube, Instagram, Telegram and Twitter (X) to distribute recruitment videos that depict life in the areas they control as ideal and in line with certain religious principles. Another example is that terrorists often use online forums and the dark web to discuss strategies, provide technical training, and distribute documents or manuals on making weapons and bombs.

Terrorism has a broad impact not only on society, but also on the Indonesian government, covering various aspects, such as psychological, social, economic and political aspects. Viewed from a psychological aspect, acts of terrorism cause people to have a deep sense of fear, not only individually but in society in general. This prolonged fear can then disrupt society's emotional stability and trigger collective stress, especially when acts of terror occur repeatedly. From a social aspect, the perceived impact of terrorism, for example, causes polarization in society, where certain groups become targets of stereotypes, discrimination or stigma, thereby destroying social harmony. This impact is exacerbated by propaganda that spreads hateful narratives or reinforces divisions.

Furthermore, from an economic aspect, acts of terrorism cause large financial losses, such as damage to infrastructure, decreased investment, and disruption of daily economic activities, while in the long term, uncertainty due

to terrorism can damage the business climate and reduce investor confidence in the stability of the country. Then from a political aspect, terrorism is of course the same as challenging the government's ability to maintain security, which can reduce public trust in state institutions. In fact, the government has made every effort possible, for example by implementing stricter security policies, which despite these policies must limit a person's freedom and are considered to reduce human rights.

From the various explanations above, in essence, through knowledge in the field of criminology, society can not only understand the direct impact of acts of terrorism, but can also take into account the long-term effects that can weaken the social structure and national stability, so that it can it is said that criminology provides the basis for the development of more effective prevention and mitigation strategies to protect society from the threat of terrorism.

Analysis of the Three Cases through Sociogenic Theory

Case 1: Abdul Azis (Imam Samudra) - Cyber-Propaganda for the Bali Bombing

This case is a near-perfect illustration of Sociogenic Theory.

a. Root Causes in Social/Political Pressures: Imam Samudra was radicalized in an environment influenced by global jihadist ideology, which frames certain political actions (e.g., Western influence in Muslim countries) as oppression. His actions were rooted in a perception of social and political injustice against the global Muslim community.
b. The Role of Social Interaction and Group Dynamics: He was not a lone actor. He was part of the Jemaah Islamiyah terrorist network. His radicalization and involvement were products of intense interaction within this group, which provided a shared identity and purpose.
c. Indoctrination through Propaganda and Ideology: His use of the internet for "provocation and propaganda" is a direct example of this point. He was both a consumer of extremist ideology and a producer, using cyberspace to instill those same values in others, continuing the cycle of radicalization.
d. The Emergence of Cyberterrorist Behavior: His cyber-activities were a logical extension of his indoctrination. The online propaganda was a tool to support the physical terrorism, demonstrating how the group's ideology seamlessly incorporated modern technology into its methods.

Case 2: WannaCry Ransomware Attack on Hospitals

This case has a weak or indirect link to Sociogenic Theory, as its primary motive was financial gain, not ideology.

a. Root Causes in Social/Political Pressures: The perpetrators were likely motivated by profit, not political alienation or injustice. There is no evidence this was an ideologically driven group seeking social change.
b. The Role of Social Interaction and Group Dynamics: While the attackers may have been part of a criminal group (like the Lazarus Group, linked to North Korea), the dynamic is more akin to a criminal organization than an ideologically-driven cell. The bonding is over profit, not a shared sociopolitical cause.

c. Indoctrination through Propaganda and Ideology: There was no ideological narrative or propaganda associated with the WannaCry attack. The only communication was a ransom note demanding payment.
d. The Emergence of Cyberterrorist Behavior: The behavior emerged from a motive of financial exploitation, not from a socially-conditioned extremist ideology. While the *impact* was terrorizing (harming critical healthcare services), the *motive* does not align with the core tenets of Sociogenic Theory as it relates to terrorism.

Case 3: Bjorka's Hack of the Ministry of Communication and Informatics
This case presents a mixed or potential link to Sociogenic Theory, depending on the unknown motive of the actor "Bjorka."

a. Root Causes in Social/Political Pressures: If Bjorka is a "hacktivist" motivated by a desire to expose government incompetence or protest specific policies, this point could apply. The pressure would be political alienation or a perception of governmental failure, driving the actor to retaliate.
b. The Role of Social Interaction and Group Dynamics: This is unclear. Bjorka could be a lone wolf or part of a collective. If part of a group with a shared anti-government or transparency agenda, this point would be relevant. The social reinforcement of the group would shape and justify the criminal behavior.
c. Indoctrination through Propaganda and Ideology: Bjorka's actions were accompanied by public statements and leaks, which can be seen as a form of propaganda to shape public opinion and expose vulnerabilities. This aligns with the theory if the goal is to instill certain values (e.g., distrust in the government, the need for better data security) in the wider society.
d. The Emergence of Cyberterrorist Behavior: The hack is the resulting behavior. If driven by sociopolitical motives (as opposed to pure financial gain or notoriety), then the act is a direct outcome of the actor's ideological framework and desire to create a social or political impact, which fits the theory.

Simply put, it can be said that in the above cases: sase 1 (Imam Samudra) is a classic example of Sociogenic Theory in action; case 2 (WannaCry) is primarily a criminal act that falls outside the theory's core focus on ideological terrorism; and case 3 (Bjorka) sits in a grey area, where the theory is applicable *only if* the underlying motivations are sociopolitical, making it a potential example of modern, ideologically-driven cyber-activism. Although in the three cases analyzed, there are gray areas in determining the definitive application of Sociogenic Theory, they have at least provided an overview that every act of terrorist evil committed via the internet displays certain motives that form the basis for criminological examination.

CONCLUSIONS AND RECOMMENDATIONS

The criminological aspect has a very important role in understanding the strategy and propaganda of terrorism via the internet. Terrorism in Indonesia has a long history and continues to develop today along with the development of

very sophisticated technology. Terrorism, which was previously only carried out through weapons, is now possible to carry out only using sophisticated technology, one of which is through the internet network, which is called cyber-terrorism. This phenomenon not only causes direct impacts such as loss of life and material, but also has long-term impacts on aspects of society's psychology, social harmonization, economic stability, and even political trust in the government. In the criminological aspect, it is direct, such as loss of life and material, but also has a long-term impact on the psychological aspects of society, social harmonization, economic stability, and even political trust in the government.

In the criminological aspect, acts of terrorism can be analyzed through Sociogenic Theory, where criminal behavior, including those involved in terrorism, is not an instant desire but is influenced by the social environment and group interactions. The motivation of terrorists is rooted in social factors and group interactions. The motivation of terrorists is rooted in ideological, political, social and psychological factors, which are often reinforced by digital propaganda via the internet. The perpetrator's strategy of using social media and online forums to spread radical narratives, recruit members and spread fear is an adaptation of terrorist perpetrators to technological developments.

Although in the three cases analyzed, there are gray areas in determining the definitive application of Sociogenic Theory, they have at least provided an overview that every act of terrorist evil committed via the internet displays certain motives that form the basis for criminological examination. Therefore, public knowledge using a criminological approach is very important in the context of prevention and mitigation strategies that are not only effective in dealing with immediate threats but also prevent long-term impacts that can damage national stability.

ADVANCED RESEARCH

This study only reveals a few criminological aspects of terrorism through the internet. There are limitations in terms of primary data collection, including in the development of a broader theory. Therefore, further research is needed to deepen the study of this issue. This study serves as a trigger for further research in the future.

ACKNOWLEDGMENT

We would like to express our deepest gratitude to all individuals and LPPM Universitas Proklamasi 45 Yogyakarta who have contributed to the completion of this research. Furthermore, we extend our thanks to our colleagues for their stimulating discussions and technical assistance. Lastly, we acknowledge the participants of this study, without whom this research would not have been possible.

REFERENCES

A. A. S. Introduction to Criminology. Makassar: Reflection Library, 2010.

A. B. A.S, & Fitriana, I. "Cyberterrorism: A Challenge of Asymmetric Communication for National Resilience," Inter Komunika: Jurnal Komunikasi, 2(1), 1–15, 2017. doi: 10.33376/ik. v2i1.12.

Admin. "10 Examples of Cyber Crime Cases that Can Be Lessons Learned," Lintasarta Cloudeka. Available at: https://www.cloudeka.id/id/berita/web-sec/empat-kas-cyber-crime/

Admin. "Examining Trends in Terrorism in Indonesia from Time to Time and How to Handle It." Faculty of Social and Political Sciences, University of Indonesia. Available at: https://fisip.ui.ac.id/menelaah-tren-terorisme-di-indonesia-dari-masa-ke-masa-dan-cara-penanganannya/

Admin. "Mariott Hotel Bombing." Wikipedia. Available at: https://id.wikipedia.org/wiki/Pengeboman_Hotel_Marriott_2003

Ashie, L. "An Analysis of Globalization as a Catalyst for International Terrorism." Semantic Scholar. Available at: https://www.semanticscholar.org/paper/An-Analysis-of-Globalization-as-a-Catalyst-for-Ashie/a97929e0a06a5141346146d01e5445c0da34d97b

Danastri, M. A. Cyber Terrorism in the Perspective of the Anti-Terrorism Law and the Information and Electronic Transactions Law. Jakarta: Jakarta Labshool High School, 2011.

Edrisy, I. F. Criminology. Bandar Lampung: Media Heritage, 2023.

Garadian, E. A. "Darul Islam (DI)/Indonesian Islamic Army (TII)." ESI Kemendikbud. Available at: https://esi.kemdikbud.go.id/wiki/Darul_Islam_(DI)/Tentara_Islam_Indonesia_(TII)

Hadjon, P. M. Legal Protection for the Indonesian People. Surabaya: Bina Ilmu, 1987.

Hutabarat, A. Y. A., & Larasati, N. U. "Analysis of Indonesian Women's Terrorist Motivation Seen from the Perspective of Differential Identification Theory," Jurnal Ilmu Kepolisian, 17(3), 1–18, 2023. doi: 10.35879/jik. v17i3.407.

Jenkins, B. M. International Terrorism: The Other World War. California: St. Martin Press, 1990.

Lutfi, H., Baharudin, & Anggalana. "Law Enforcement Analysis of Misuse of Village Funds in Village Development," Jurnal Al-Ilm, 4(1), 12–28, 2022.

MacDonald, J. J. P. L. E. “Cyber Terrorism: A Study of The Extent Coverage in Computer Security Textbook,” Journal of Information Technology Education, 3, 280, 2004.

Martien, D. Legal Protection of Personal Data. Makassar: Science Partners, 2023.

Martin, R., & Hamonangan Pasaribu, A. "Shooting Actions in the Police Headquarters as a Form of Women's Involvement in Terrorism," Jurnal Kewarganegaraan, 6(1), 2176–2181, 2022.

Mildawati, T. "Information Technology and Its Development in Indonesia," EKUITAS (Jurnal Ekonomi dan Keuangan), 4(2), 101–110, 2000. doi: 10.24034/j25485024.y2000.v4. i2.1904.

Muhaimin. Legal Research Methods, Print I. Mataram: Mataram University Press, 2020.

Muhaimin. Legal Research Methods. Mataram: Mataram University Press, 2020.

Mumtaaz, G. M., Wardhana, R. T., & Fibiya, H. D. "Al-Hakam Islamic Law & Contemporary Issues," Al-Hakam Islamic Law and Contemporary Issues, 2(2), 48–59, 2021. Available at: ejournal2.undip.ac.id

Munthe, M. G. "Propaganda and Communication Science," Jurnal UMN, IV (1), 40–50, 2012. Available at: https://www.researchgate.net/publication/328044738_Propaganda_dan_Ilmu_Komunikasi

Nurudina, S. "Critical Analysis of Terrorism Propaganda Narratives Through Online Media," Innovative Journal of Social Science Research, 4(4), 5521–5532, 2024. Available at: http://j-innovative.org/index.php/Innovative/article/view/12347

Online Legal Team. "Terrorism: Definition, Causative Factors, and Types." Hukumonline. Available at: https://www.hukumonline.com/berita/a/terorisme-dapat-lt6183b09848f15/?page=3

P. RH. "Indonesia is the First Time to Dismantle a Case of 'Cyber-Terrorism'," Antara News. Available at: https://www.antaranews.com/berita/42142/indonesia-pertama-kali-besar-kas-cyber-terrorism

Rahardjo, S. Other Sides of Law in Indonesia. Jakarta: Kompas, 2003.

Respati, R. R., Wahyurudhanto, A., & Dharma, S. "Policing Strategy for Preventing Terrorism Crimes," Jurnal Ilmu Kepolisian, 14(3), 189–209, 2020. doi: 10.35879/jik. v14i3.279.

Rizki, M. J. "Seeing Terrorism Movements Through 'New Media'," Hukumonline. Available at: https://www.hukumonline.com/berita/a/mebayaran-terorisme-via-new-media-lt665d2405587e1?page=2

Rumadan, I., & Ridwan, M. Terrorism and Jihad Legal and Social Religious Review. Ambon: Student Library, 2020.

Sari, D. R. "Regulation of Supervision Criminal and Social Work Criminals in the Draft Criminal Code as an Effort to Implement Daad-Dader Strafrecht," SALAM: Jurnal Sosial dan Budaya Syar-i, 9(1), 133–140, 2022. doi: 10.15408/sjsbs. v9i1.24338.

Sugiono, S. "Radicalism in the Family," Religious Social Bulletin, II, 2017.

Susanti, E., & Rahardjo, E. Law and Criminology. Bandar Lampung: CV. Anugrah Utama Raharja, 2018.

Susanto, I. S. Criminology. Yogyakarta: Genta Publishing, 2011.

Tysara, L. "What is ISIS? Understand the history and factors causing its spread in ASIA," Liputan6. Available at: https://www.liputan6.com/hot/read/5317671/apa-itu-isis-pahami-histori-dan-besar-besar-besarannya-di-asia

Yusuf, O. "Indonesian Hospitals Become Victims of 'Cyber Terrorism'," Kompas. Available at: https://tekno.kompas.com/read/2017/05/13/17180077/rumah.sakit.indonesia.jadi.korban.terorisme.cyber