

Strengthening the Cyber Terrorism Law Enforcement in Indonesia: Assimilation from Islamic Jurisdiction

Muammar Bakry^{1,*}, Abdul Syatar¹, Achmad Abubakar¹, Chaerul Risal¹, Ahmad Ahmad¹ and Muhammad Majdy Amiruddin²

¹Faculty of Sharia and Law, Universitas Islam Negeri Alauddin Makassar, Indonesia

²Faculty of Islamic Economics and Business, IAIN Parepare, Indonesia

Abstract: The threat of terrorism is exacerbated by technology. It leads to a new term called Cyberterrorism. Apparently, this threat has not received appropriate space in the legal regulations in Indonesia. Therefore, this paper aims to strengthen legal action against cyberterrorism. This strengthening is obtained by assimilating Islamic law through the normative juridical method. The data are sourced from related news and updated journals. Researchers found that the assimilation of Islamic law products into positive law in Indonesia was in the form of Hirabah Punishment, Rebel Punishment, or Takzir. This idea is expected to be a consideration for policymakers in updating their laws so that they can reduce terrorism crimes, especially in cyberspace.

Keywords: Cyber terrorism, Islamic Jurisdiction, The Law Enforcement.

INTRODUCTION

The accelerated evolution of technology has made the crime of terrorism more massive and structured. The crime of terrorism is growing no longer in a traditional form but utilizing internet technology to spread its actions (Astuti, 2015). Public facilities based on information and electronic technology have the potential for terrorism crimes to emerge, which also use information technology facilities and are very vulnerable to occur in Indonesia. It leads to a new form of terrorism that uses or uses information technology, commonly known as Cyber Terrorism (Adam, 2014). The threat of cybercrime can only be reduced but cannot be eliminated absolutely (Sampath Kumar Venkatachary, 2018). In general, the threat of cybercrime in Indonesia is a crime in an increasingly worrying digital society. For example, in the 2013 State of the Internet report, Indonesia was mentioned as the second country in cybercrime in the world (Sugihartati, 2020).

Tito Karnavian, former Chief of the Indonesian National Police, explained that currently, the terrorist perpetrators are recruiting members and training to assemble bombs through social media. Terrorists are also looking for funds through bitcoin. Cyber terrorism and cyber jihad do recruitment and training. Exercises are no longer physical, but online, how to make bombs (Hidayat, 2016). The first cyber-terrorism case uncovered in Indonesia was a criminal case involving the perpetrator on death row in the 2002 Bali bombing,

namely Abdul Azis alias Imam Samudra (Priyambodo, 2006). The new phenomenon of cyber terrorism in the form of the WannaCry ransomware attack is widespread throughout the world, including Indonesia. The malicious program has taken hostage computer systems of several hospitals, making it difficult for medical services to patients. As a result, it is difficult for patients to queue (Yusuf, 2017). These cases show that cyber terrorism is increasingly prevalent in Indonesia. Certain groups make use of the internet network to carry out terror against the public or the government. Terror is carried out through piracy, theft, and destruction of data on computer systems so that important information cannot be used.

The traditional terrorist attack planning cycle and later cyber-terrorist planning are used to penetrate the network system (Neely, 2018). Terrorists are widespread in the media as a sophisticated means of communication, thus enabling more extraordinary acts of terrorism (Neely, 2018). Acts of terrorism experience shifts and changes in patterns and forms. They do this to follow the pattern of social and political developments that occur. These changes were also carried out in response to information media and communication patterns and community relations (Rochmawati, 2016). As an example of a terror threat, ISIS claims that its group still exists and can carry out cross-border operations. ISIS has intensified guerrilla operations and terrorism in various transcontinental countries. As an illustration, the group's potential threat of terrorism by the group is still a severe problem for international security (Wibowo & Hapsari, 2020). Cyber terrorism is detrimental to individuals and institutions and even countries, including those who feel the

*Address correspondence to this author at the Faculty of Sharia and Law, Universitas Islam Negeri Alauddin Makassar, Indonesia;
E-mail: muammar.bakry@uin-alauddin.ac.id

impact. Cyberlaw is needed to prevent radicalization on social media. So that acts of terrorism can be prevented by the security apparatus (Marpaung *et al.*, 2017). The majority of countries in the world already have laws in place to deal with cybercrime, America uses Uniform electronic Transaction (UETA), Singapore uses The electronic Act (Electronic deed) 1998, electronic Communication Privacy Act (Electronic Communication Privacy Act) 1996 (Marpaung *et al.*, 2017). So rampant cyber terrorism in Indonesia that handling it needs special attention from the government, especially the State of Indonesia, which unexpectedly has a high crime rate in cybercrime.

Thus, a strict law is needed to target their actions through internet media. The target of cyber terrorism is very detrimental to the party being attacked and will cause tremendous discomfort and fear. The motive used in cyber-terrorism is to cause fear in the community, spreading propaganda using the internet can spread better and faster, tapping is for the benefit of which is organized. It can cause huge losses, gathering information to spread fear in the community, and as a means of effective and safer communication (Rochmawati, 2016)

The efforts of terrorists in exerting pressure on society is through actions in cyberspace. Crimes related to ideology and brainwashing of ideas against the sovereignty of the Indonesian State are committed by using communication media with technological means. Indonesia as a rule of law that seeks to develop regulations in handling technology and information crimes, especially those related to acts of terrorism through cyberspace networks. The government should pay attention to strengthening the law related to terrorism crimes in deciding the perpetrators' actions.

Cyber terrorism projects are new toys for terrorists to achieve their objects. Cyber terrorism is considered economical and more efficient than the old-style often used by terrorist groups so far. Cyberterrorism can attain a broader area than the old style. Cyberterrorism activities do not require formal training, such as the military. Moreover, the resulting impression can be more potent than the usual method (Putra, 2020).

One of the negative consequences of Cyberterrorism is its ability to praise internet users with misinformation and misleading views. This information leads to deviations from the agreed terms of religion and obscures the proper meaning so that users are led

to believe their proposals. Many of these users decided to join. Approach models can vary along with the variety of platforms offered by the internet, ranging from websites, videos, social media, and instant chat media. Cool and contemporary packaging plays an increasingly important role in capturing the attention of internet users. Cyber terrorism has the ultimate goal of terrorism propaganda to radicalize civilization. Radicalization that occurs through internet media can occur separately and integrated with the natural world (self-radicalization or self-radicalization). It means that someone can convert to radical wherever they are, without even dealing undeviatingly with radical groups such as preaching. A person can convert radicalized even when he reaches distorted information through the internet in Indonesia.

Islam strongly condemns acts of terrorism in various forms, both traditional and through cyber media internet. Therefore, it is exciting to conduct a comparative study between the criminal system in Indonesian law and Islamic criminal law regarding cyber-terrorism. No religion or state teaches acts of terror in various forms. The perpetrators of these acts of terrorism often happen to be Muslims, giving a bad image to Islam itself. Islamic criminal law is stringent in handling and following up terrorism crimes itself

METHODOLOGY

This study uses a qualitative method that combines the relevance of criminal sanctions in the Indonesian legal system and Islamic criminal law. It does not explicitly provide legal rules regarding cyber-terrorism crimes as a legal umbrella in Indonesian criminal law. However, perpetrators of cyber terrorism are still accused by the Terrorism Law and the ITE Law only. Cyber terrorism is a critical study in new media in acts of terrorism. The approach used is normative and juridical, both in Indonesian legislation and Islamic criminal law. Primary data is obtained from credible and update literature, such as laws and regulations, court decisions, books/books and reputable journals. Secondary data is found from supporting information such as websites and the like and then presented with a robust analytical instrument based on normative arguments

LITERATUR REVIEW

The Origin of Cyber Terrorism

Barry Collin first introduced the term cyber terrorism in 1997, a senior researcher at the Institute for Security

and Intelligence in California, United States. In Barry Collin's view (Denning, 2000), computerization in various areas of human life creates new vulnerabilities. This vulnerability can be exploited for acts of terrorism either through destruction (destruction), alteration (alteration), and acquisition and retransmission (acquisition and retransmission), the purpose of which is to cause chaos and terror.

The virtual world is a virtual world that is formed from the union between humans and technology. According to Koops (Astuti, 2015), technology functions are to store, transmit, and process information and technology. The impact of technological developments has led to the development of cyberspace, giving birth to the development of the ideology of freedom in the cyber world. Ideological initiators also take advantage of the internet world to launch terrorism, freedom to convey information that includes competing against one another and slander, and argues with the liberty to launch creativity to destroy and spread the virus of terrorism.

Cyber terrorism is a form of cybercrime. In terms of the concept of cyber terrorism, it is not much different from conventional terrorism. It is just that there is an element of "cyber" here. Some researchers argue that terrorist activities in cyberspace are considered cyber terrorism (Ahmad & Yunus, 2012).

On the other hand, cyber terrorism is a form of structured and planned crime that is politically motivated in the form of attacks on information, computer systems, computer programs, and data to result in considerable losses and the fall of innocent victims by a group or individual. By extension, the internet and social media can also spread radical ideas to disturb society (Putri & Wahyudi, 2019). Propaganda is a crucial initial stage in influencing perceptions and attracting public attention, manipulating subconscious thoughts, and directing one's actions to follow the goals to be achieved.

Cyber terrorism is a form of development of cybercrime and terrorism. There are two aspects of cyber terrorism: cyberspace and terrorism, which combine two criminal acts. The perpetrator is called cyber terrorism. Hackers and crackers can also be called cyber terrorism because the activities and activities they carry out in cyberspace can often terrorize and cause significant harm to the victims who are their targets, like "conventional" acts of terrorism. The definition of cyber terrorism put forward by James

A. Lewis defines cyber terrorism as using computer network devices to shut down crucial national infrastructure (such as transportation and energy sources) or disturb and intimidate a government or group of citizens. International crime tends to be a particular crime phenomenon that occurs across national borders, subject to two or more state jurisdictions (Hiariej, 2009). In the Ratification of the ASEAN Convention on Counter-Terrorism, several provisions are stipulated. The establishment of this convention is based on the commitment of ASEAN countries in eradicating terrorism in Article VI (j): "Strengthen capability and readiness to deal with chemical, biological, radiological, nuclear (CBRN) terrorism, cyber terrorism and any new forms of terrorism;" All countries must be prepared to prevent acts of terrorism and work together to increase public awareness in eradicating terrorism in all things, including cyber terrorism. The Indonesian state has also ratified the ASEAN Convention on Counter-Terrorism, as stated in the ratification of Law Number 5 of 2012 concerning the ASEAN Convention on Combating Terrorism.

Cyberterrorism is a part of cybercrime, which is included as a transnational crime (Kadir *et al.*, 2019). The potential threat of cyber terrorism in Southeast Asia is relatively high due to economic growth (Ramadhan, 2019). The development of these crimes requires limitation and accountability from crimes with the use of technological tools (Astuti, 2015). Today's threat of terrorism has grown in the digital world, marked by the massive use of technology. In the end, cooperation between governments, the private sector, and the public are needed to identify, communicate, and deradicalize as efforts to deal with the problem of terrorism that has penetrated cyberspace (Putri, 2019).

Cyber Terrorism in Indonesia

Fahrul Razi, former Minister of Religion of the Republic of Indonesia, has the task of dealing with radicalization in Indonesia after being inaugurated in October 2019 (Setyawan, 2019). This task is an indication that parties are spreading radical ideas and terrorism in Indonesia (Asrori, 2015). Even more astonishing is the development of terrorism crimes through efforts to spread radicalism and online sites that the government blocks, such as www.arrahmah.com (Siagian & Sumari, 2015). With this phenomenon, terrorism and radicalization have become the central discourse because they serve as an analytical paradigm to interpret the phenomenon of violent jihadist terrorism (Malthaner, 2017).

The threat of cyber terrorism can befall all countries, including Indonesia. The application of internet facilities to carry out terrorism needs to be aware of its movements. Almost all vital state-owned facilities and public facilities today utilize and depend on internet technology because of its speed and flexibility in providing information quickly and can connect all things.

Indonesian people enter international relations through internet media with technological advances as part of changing communication patterns. Technological progress is marked by hardware such as computers and laptops, along with software. As a result of this hardware, terror actors also use it to carry out their acts of terror through the internet world. Thus, the cyber-terrorist act creates social problems that are far more developed and globalized with the resulting impact. Technology forces the terrorists to launch their actions in virtual reality.

Cyber terrorism attacks can penetrate anything connected to the internet, especially vital government objects that can interfere with its function and even make more significant victims than terrorism carried out in conventional ways. There are no specific laws and regulations in Indonesia that regulate cyber terrorism, which creates legal uncertainty because if the crime occurs in Indonesia. Many people question what legal basis should be used in ensnaring the perpetrators of this crime. It is in line with article 1 paragraph (1) of the Criminal Code, which reads, "An act cannot be convicted, except based on existing statutory provisions" (Adam, 2014). However, this principle does not mean that it does not interpret the formulation of offenses in the statutory regulations. So that if there is a criminal act of cyber terrorism, an interpretation can be made of the existing laws and regulations related to this crime, in this case, namely Law Number 5 of 2018 concerning Eradication of Terrorism and Law Number 19 of 2016 concerning Information and Information—electronic Transactions.

This cyber terrorism incident has also occurred in Indonesia, namely, the WannaCry Ransomware attack, which has spread widely throughout the world, including Indonesia. The malicious program has even taken hostage computer systems in several hospitals in Jakarta, thus hampering medical services and patient data access. Director-General of Applications and Information at the Ministry of Communication and Information, Samuel Abrijani Pangarepan, called the ransomware attack a form of cyber terrorism. Hospital

complaints are related to the queuing computer system for patients who have stopped working because they are infected with ransomware; not only hospitals in Indonesia are victims of this malicious program because WannaCry has spread to nearly 100 countries worldwide. Doctors have difficulty accessing patient medical records because their computers are locked. Hundreds of computers infected with WannaCry itself spread randomly, quickly, and widely. However, some of the victims happened to come from negligent and missed prevention hospitals, such as updating the operating system. This ransomware also attacks other institutions from various sectors, from transportation to telecommunication around the world. The queuing system is connected to all hospitals, and all national referral hospitals are connected to a network of the Ministry of Health. WannaCry uses the NSA cyber weapon tool leaked by hackers to automatically infect victims' computers without the need for human intervention. Once inside, this ransomware will lock data and computer systems so that it cannot be accessed Yusuf, "Rumah Sakit Indonesia Jadi Korban terrorism Cyber."

The application of positive law in Indonesia against cyber terrorism must be maximized. Currently, the Indonesian state has focused on eradicating extraordinary crimes, including corruption, narcotics, and terrorism, which are considered cancer that can eat away and destroy Indonesia in a relatively long period, but not only that. Crimes that are not extraordinary and can destroy Indonesia instantly or in a relatively short period, namely cyber terrorism. Cyber terrorism can destroy Indonesia in an instant. Indonesia is so dependent on the development of technology and information. It reaches the country's vital tools such as confidential data information, electricity distribution, use of communication tools, military equipment controlled through technology and other virtual systems so that it can cyber terrorism criminals use as tools or media to carry out their actions.

According to the Counter-Terrorism Task Force of Council of Europe, there are several reasons why terrorists use the internet as a medium for carrying out terrorist activities. Attacks can be carried out from anywhere globally; attacks can be carried out quickly; for example, worms and viruses can spread widely without the need. In the presence of further perpetrators' involvement, Internet attacks can be disguised by specific programs or techniques, making them difficult to trace, and using the internet is cheaper.

The 21st century has brought humans to the advances of life and civilization, along with advances in science and technology. With advances in communication and information technology, globalization has increased the interconnection between humans almost without borders of countries and regions. The 21st century is marked by the information and information revolution. This development brings hope for a better, more peaceful, and prosperous human life. Globalization, accompanied by an information revolution, should facilitate the development of shared understanding and a sense of brotherhood in a relationship of universal responsibility to create a world society that is "civilized society" and "decent society" (Kaligis, 2012).

The reality is not so. This development presents a complexity of problems. Humans are faced with various kinds of conflicts and the threat of conflict. John Reid, United States Secretary of State for Defense, in his speech on April 3, 2006, at the Royal United Services for Defense and Security, revealed that the threats we face today are different and significantly more complicated than before. The threats to the future are more uncertain and include ecological, economic, and political issues and social (Kaligis, 2012).

As a social engineering tool, the law must be used to provide a way for developments in society, especially for developments in technology. For this reason, the regulation of technology transfer is a measure of a country's progress (Kaligis, 2012).

The target of cyber terrorism is indeed very detrimental to the party being attacked and continues to cause discomfort and fear. The motive used in cyber-terrorism is to cause fear in the community. Spreading propaganda using the internet can spread better and faster. Tapping is for organized interests. and can cause enormous harm, gathering information to spread fear in the public means of effective and safer communication (Rochmawati, 2016). Usually, the number of targets resulting from cyber-terrorism crime activities is more significant because the perpetrator can break into computer access or individual or public accounts Hendriyanto Kusno Jacob, 'Peranan Penyidik Dalam Tindak Pidana Cybercrime,' VI.6 (2017), 124–31. *Cyber terrorism can target computer networks belonging to individuals, governments, communities, private airlines, and likes. The complexity of selecting targets or targets allows terrorists to find weaknesses that they can continue to exploit* (A.S & Fitriana, 2009).

The advancement of terrorist groups in Indonesia is within investigations, recruitment of cadres and military discipline, and propaganda. The propaganda content is mostly to blame for government enforcement and ventures that does not accommodate their idea. Furthermore, their propaganda does not have a valid argument base and seems to ambush the government's authority and legitimate power. Their critical actions are not accompanied by a polite and legal approach but rather towards violence and terror. New recruitment members will be given basic training called 'I'dad or preparation. They were first provided with the motto, "there is no jihad without I'dad. This training has the same pattern as military training in general. In 2010, the same training was adopted in Aceh. They were given the training to utilise firearms. The group was finally arrested and treated legally (Putra, 2020).

RESULTS

The Law Enforcement of Cyber Terrorism in Indonesian Legal System

In Indonesia, the prevention of cyber terrorism is a priority that must be eradicated and overcome. The government is countering radicalism propaganda through internet media by establishing procedures that are disputing and manageable advances Rigid approach policies in part termination, domain registration revocation, IP address filtering, data selection, and search engine working mechanisms. This responsibility belongs to various authorities' collaboration, ranging from the central government, regional governments, and related ministries. It is just that these efforts have not been effective in stemming terrorism attacks via the internet. the many conflicts of interest and the lack of cooperation are the scapegoats for this failure. The government is seen as opposing Islamic situations (Nadjib & Cangara, 2017).

The Indonesian authority has declared a course in a moderate strategy to overcome this intricacy. These courses incorporate counter-ideology, counter-propaganda, and counter-narrative by appropriating communications literacy (Sari, 2017). Communication literacy is the community's capacity to obtain, investigate, and present the message for individual results. Communication literacy indicates a person's ability to think critically and evaluate knowledge derived from the mass media. Communication literacy is an option to licensing schemes that are said to restrict the right to information.

The regulation regarding Cyber Terrorism crimes has not been clearly and firmly regulated in the legislation in Indonesia. In particular, in Law Number 5 of 2018 concerning Amendments to Law Number 15 of 2003 concerning Eradicating Criminal Acts of Terrorism and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. However, law enforcement officials can still use the existing legal provisions, given the lengthy process required to prepare legislation. Positive law in Indonesia is still fragile to ensnare the perpetrators of cyber terrorism. What is meant here is concrete and precise regulation by not including and pouring the word of Cyber terrorism into both laws to create uncertainty and a legal vacuum against cyber terrorism.

In-Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism, cyber terrorism can be charged under Article 13A. Anyone who has a relationship with a terrorist organization and deliberately spreads words, attitudes, or behavior, writing, or displays to incite a person or group to commit violence or threats of violence that can result in a criminal act of terrorism punishable by a maximum imprisonment of five years. Although this article does not explicitly mention internet networks as a medium used in spreading terrorism, this article is closer to and inclined towards cyber terrorism.

Whereas in using the approach of Law Number 19 the Year 2016 concerning Electronic Information and Transactions in ensnaring cyber terrorism perpetrators, the article that can be used is Article 45A Number 2, which reads "Anyone who deliberately and without rights spreads information aimed at causing hatred. Alternatively, confident individual and community group hostilities based on ethnicity, religion, race, and inter-group (SARA), as referred to in Article 28 paragraph (21) shall be punished with imprisonment for a maximum of 6 (six) years and a maximum fine of IDR 1,000,000,000.00 (one billion rupiahs).

Law Number 19 of 2016 concerning Electronic Information and Transactions is a law that regulates cybercrime in a broad sense, while cyber terrorism itself is a part/type of cybercrime. The methods or methods used in handling crime this has been regulated in this law. To entrap cyber terrorism perpetrators by using Law Number 5 of 2018 concerning Eradication of Criminal Acts of Terrorism and Law Number 19 of 2016 concerning Electronic Information and Transactions. It can be used as limited

as articles that can support or are compatible with one another. However, both laws still have shortcomings and weaknesses, such as not providing a grammatical definition of cyber terrorism. Almost all articles can be applied to protect against cyber terrorism, especially internet users. Law Number 11 of 2008 concerning Electronic Information and Transactions is a law that regulates technology-based crimes (cybercrime), while cyber terrorism is a part/type of cybercrime so that the methods or methods used to commit the criminal act has been regulated in this law Rezqi Endah Sari Nurul, Fitriati Fitriati, and Seprasia Rianda, 'Pengaturan Terhadap Cyber Terrorism Dalam Hukum Pidana Indonesia' (Universitas Bung Hatta, 2020).

The evidentiary effort to find out that a person or group of people has the intention and plan of committing a crime of cyber terrorism, of course, the investigator must obtain evidence to support the allegation if it turns out that there intends to commit a criminal act of terrorism. The provisions of Article 27 of Law Number 15 the Year 2003 have stated various kinds of evidence. One of them mentions electronic evidence as parallel and valid evidence as referred to in the Criminal Procedure Law.

Such proof is also stated in the provisions of Article 184 of the Criminal Procedure Code that the information uttered, sent, stored electronically by using an optical instrument can be issued with or without any means, whether written on paper, any physical object other than paper. Recorded electronically, including but not limited to writing, sound or images, maps, designs, photographs, or the like, letters, signs, numbers, symbols, or perforations that have meaning or can be understood by those who can read or understand them.

The ITE Law is the first cyber law in Indonesia that regulates information and electronic transactions explicitly after the previous telecommunications law. The ITE Law material can be grouped into 2 (two) major parts, namely the regulation of information and electronic transactions and the regulation of prohibited acts (cybercrime).

According to Josua Sitompul (Sitompul, 2012) The provisions of cybercrime in the ITE Law refer to the EU Convention Cybercrime (CoC), an international instrument used by many countries. The CoC regulates two types of cybercrime. First, in the sense of regulated computer crime, cybercrime is a crime aimed at the confidentiality, integrity, and availability of data and computer systems and included in this category are

illegal access, illegal interception, data interference, system interference, and misuse of devices. Second, cybercrime in the sense of the computer-related crime. This scope is a computer-related forgery and computer-related fraud.

The development of cybercrime forms is high-speed, along with the development of information technology based on computers. The ITE Law and the Draft Law (RUU KUHP) have responded with cyber law enforcement efforts. In law enforcement against criminal acts of cyber terrorism, law officials and judges as justice providers should be able to use the provisions of the ITE Law and the Criminal Code following the crimes committed so that the justice desired to protect the state and citizens can be achieved.

Cyber terrorism is declared an extraordinary crime. All countries highlight this crime that impacts state security disturbances, and everyone who becomes a citizen does not feel safe and calm by terrorist crimes that have begun to invade cyberspace. The crime of terrorism is an extraordinary crime because the nature of terrorist crime is now moving to carry out its actions beyond state boundaries and organized (transnational organized crime).

Assimilation of Cyber Terrorism Legal Law from Islamic Jurisdiction

Recently, the strengthening of the radical Islamic movement is a fact that has occurred in Indonesia (Susanto, 2018). The phenomenon of terrorism in the name of Islam in various ways, for example, employing a suicide bombing, is disconcerting to the community and has developed into cyber-terrorism. Many parties criticized and blamed Islam for the incident because the action was a struggle to defend religion or, in other words, "jihad" by the perpetrators (Rahman, 2018). Terrorism is not given space in Islam because Islam does not teach violence. Therefore terrorism cannot be linked to the term jihad taught in Islam; Islam's primary mission is *rahmatan lil'alam*.

In Indonesia, radical groups spread Islamic radicalism globally. They actively propagate and maintain a global fundamentalist identity and, at the same time, build a local-national identity. In the context of mobilizing religious groups' interests, the internet is seen by its users as a very strategic, effective, efficient, economical, and fast vehicle (Nasrullah, 2012).

Terrorism in various forms is unknown in Islam because Islam does not teach violence (Rahman,

2018) Therefore, terrorism cannot be linked to the term jihad taught in Islam, the main mission of Islam is *rahmatan lil'alam* (Handoko, 2019). Islam is not a primitive religion, but an advanced religion and can solve problems that have occurred over time until now (Rachman, 2018). Terrorism as an understanding is different from most of the understandings that have grown and developed in the past and present. Terrorism is always synonymous with terror, violence, extremism, and intimidation. The perpetrators are usually referred to as terrorists. Terrorism, as an understanding that is synonymous with terror, often has harmful and destructive consequences for humanity (Wajdi, 2017).

Acts of terrorism are a configuration of planning crimes to achieve specific goals, both political and economic (Arake, 2013). Criminal acts in the form of cyber terrorism in general in Islamic criminal law have three possible forms of crime:

First, it can be charged with hirabah punishment (Naro et al., 2020). Hirabah, in Islamic penalties, has four criminal sanctions, namely murder, crucifixion, cross-cutting of accomplices, and exile ('Abd al-Qadir 'Audah, 2013, p. 494). These sanctions are contained in the Qur'an surah al-Maidah verse 33.

A brief explanation of the relationship between hirabah and cyber terrorism causes substantive acts of public fear. They were killed if the perpetrator of cyber terrorism crime results in killing people. The murder penalty is not called kisas but is one of the penalties in the criminal act of hirabah. The punishment cannot be forgiven by the heirs of the slain, as is the case in the kisas (Syatar & Abubakar, 2020). They were crucified to death if the perpetrator of the cyber terrorism crime results in murder and taking property. The murder sentence was not kisas because the sentence of murder and crucifixion could not be forgiven by the heirs who were killed and whose property was taken. Cut off the hands and feet simultaneously in opposite directions, if the perpetrator only took the property of the person from the act of terror. The punishment of exile, if the cyber terrorism actors commit acts of disturbing public security, do not kill and confiscate property (Syatar & Abubakar, 2020, p. 74).

Hirabah is a criminal act committed openly accompanied by violence. Hirabah is also an act of crime or vandalism using weapons/tools carried out by humans openly, whether carried out by one person or in a group, without considering and considering who acts of violence accompany the victim.

Cyber terrorism can be charged with hierarchical punishment due to the act of terror of a person or group of people within the country for committing chaos, murder, confiscation of property that openly disturbs and violates applicable regulations, humanity, and religion. Cyber terrorism facilitates communication between terrorists via the internet by developing a strategy through a particular website as a medium for coordinating all activities related to the implementation of terror actions, carrying out money laundering from the results of credit card fraud on several gambling sites and the like with the same goal, namely destruction and chaos.

The relevance of cyber terrorism and *hirābah* also lies in the process of carrying out threats, spreading radical ideas, recruiting and training terrorist members, internet-based attacks on important institutions, spreading propaganda, spreading explosives and weapons, spreading terrorism orations and scenes—the suicide bomber. The use of computer viruses, creating networked communication forums and websites that provide everything from how to use computers to hijack and make bombs to dividing beheading and suicide bomb attacks.

Second, cyber terrorism can be ensnared with acts of rebellion (Syatar & Abubakar, 2020). There is only one punishment for rebellion in Islamic penalties, namely murder ('Abd al-Qadir 'Audah, 2013). The punishment is based in the Qur'an surah al-Hujurat verse 9.

Rebellion in Islam means violating a politically legitimate government (Rustam, 2016). Thus, cyber terrorism crimes are political crimes. Political violence can be interpreted as an activity of destruction and extermination that causes harm and loss aimed at particular objects and affects the social system (Arake, 2013).

Cyber terrorism and action against the state (treason) have fundamental similarities. Perpetrators of criminal acts of cyber terrorism collaborate to develop acts of treason in a peaceful country. Their crimes are highly organized, massive and structured through internet networks such as regulating access, installing protection, monitoring attacks, firewalls, and so on that can destabilize a country caused by political disillusionment or economic inequality, according to cyber terrorists.

Third, takzir which is decided by the government. Cybercrime in Islamic criminal law is punishable by

takzir (M. Naufal & Jannah, 2012). *Takzir* is a sanction determined by the judge's carefulness in deciding a case as long as it does not exceed the outlined limit. That punishment is not explicitly regulated by the text, the Koran, and the sunnah (Al-Buti, n.d.). According to Islamic criminal law experts, the sentence in the criminal act of *takzir* is not particular about the amount of the material sentence because the sentence's determination is left entirely to the judge in a country. However, Islam offers several punishments, both those who are determined in form and number and have not been determined ('Abd al-Qadir 'Audah, 2013). *Takzir* criminal sanctions offered in Islamic criminal law are in the form of (M. Naufal & Jannah, 2012): Death penalty, if a criminal act of *takzir* is committed, can only be overcome by the penalty of suicide, like a punishment for spies and big criminals or recidivists, not more than ten lashes for those who repeatedly commit similar crimes. Imprisonment, whether limited or unlimited if according to the judge, the sentence is appropriate and following the purpose for which the sentence was prescribed. Isolation and boycott, such as for people who always disturb society's security and peace. Crucifixion, but not to be killed and still given food and opportunity to perform worship. Compensation by confiscation, warnings and advice, revocation of individual rights, Condemnation and social exclusion, disseminating news and fines.

The behavior of the perpetrators of cyber terrorist crimes impose a strategy for implementing prevention and treatment that is more relevant to the times, especially in Indonesia. Forming cyber law laws, exchanging information with other countries, revising laws that are counterproductive in the eradication of cyber terrorism. Regulatory models that can be relevant are the spirit offered by Islamic criminal law through criminal sanctions *hirābah*, rebellion (*al-bagyu*) and *takzir* which is returned to the legal government in a country.

CONCLUSION

It is undeniable that a special regulation on cyber terrorism does not yet exist, even though Indonesia already has several provisions related to cyber terrorism. However, it has not been able to cover it clearly and precisely. To what extent the actual need for cyber law as a *lex specialis* in managing cyber terrorism must be seen.

It is necessary to specifically include cyber terrorism regulation in cyberlaw provisions, which have an urgent

need to be used. One of the relevant considerations is including a bill for special rules on cyber terrorists on a priority scale. Considerations of Islamic criminal law or the spirit of Islamic criminal law can be used as input because Islamic criminal law is very harsh for crimes that disrupt society and a nation's stability. Due to the higher frequency of technology use with developing systems, with the existing convergence of media. Regulations regarding cyber terrorism in cyberlaw are expected to provide firm assurance in the legal explanation regarding the regulation of cyber terrorism crimes in particular. Of course, it has the main reason, namely the existence of aspects related to cyber terrorism, which are comprehensively emphasized in a provision of the cyber law that regulates the movement and use and deviations in cybercrime that use computers as the primary tool and benefit of technological media.

It means that it does not depend on just one law, even though we know there is Law Number 5 of 2018 on Amendments to Law Number 15 of 2003 or Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 About Information and Electronic Transactions. Indeed, juridically, in solving the legal problem of cyber terrorism, the judge in charge must make legal discovery through legal interpretation and construction. However, suppose the development of national law appreciates the presence of cyber law in an integrated manner. In that case, it will be a better strengthening of legal certainty, considering that there are many movements related to criminal acts of terrorism that are increasingly developing with various communication patterns in the benefit of existing media, as a means of communication to commit crimes.

ACKNOWLEDGEMENT

Gratitude to Allah who inspired us the passion to work through writing. We also extend our unlimited thanks to our leaders, especially to Prof. H. Hamdan Juhanis, M.A., Ph.D. which always encourages us to advance the institution through active scientific work.

REFERENCES

Journal Article

- A.S, A., & Fitriana, I. (2009). Cyberterrorism: Suatu Tantangan Komunikasi Asimetris Bagi Ketahanan Nasional. 1–15.
- A.S, A., & Fitriana, I. (2009). Cyberterrorism: Suatu Tantangan Komunikasi Asimetris Bagi Ketahanan Nasional. 1–15.
- Adam, A. J. (2014). Tindak Pidana Cyber Terrorism Dalam Transaksi Elektronik. *Lex Administratum*, 11(3), 164–173.
- Adam, A. J. (2014). Tindak Pidana Cyber Terrorism Dalam Transaksi Elektronik. *Lex Administratum*, 11(3), 164–173.
- Ahmad, R., & Yunos, Z. (2012). A dynamic cyber terrorism framework. *International Journal of Computer Science and Information Security*, 10(2), 149.
- Ahmad, R., & Yunos, Z. (2012). A dynamic cyber terrorism framework. *International Journal of Computer Science and Information Security*, 10(2), 149.
- Al-Buti, M. S. R. (n.d.). *Muhadharat fi Fiqh al-Muqaran*. Damaskus: Dar al-Fikr.
- Arake, L. (2013). *Islam Melawan Kekerasan dan Terorisme* (1st ed.). Yogyakarta: Prudent Media.
- Asrori, A. (2015). Radikalisme di Indonesia: Antara Historisitas dan Antropisitas. *Kalam: Jurnal Studi Agama Dan Pemikiran Islam*, 9(2), 253–268.
<https://doi.org/10.24042/klm.v9i2.331>
- Astuti, S. A. (2015). Law Enforcement of Cyber Terorism in Indonesia. *Rechtsidee*, 2(2), 157.
<https://doi.org/10.21070/jjhr.v2i2.82>
- Astuti, S. A. (2015). Law Enforcement of Cyber Terorism in Indonesia. *Rechtsidee*, 2(2), 157.
<https://doi.org/10.21070/jjhr.v2i2.82>
- 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.
- 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.
- Handoko, A. (2019). Analisis Kejahatan Terorisme Berkedok Agama. *SALAM: Jurnal Sosial Dan Budaya Syar-I*, 6(2), 155–178.
<https://doi.org/10.15408/sjsbs.v6i2.11041>
- Handoko, A. (2019). Analisis Kejahatan Terorisme Berkedok Agama. *SALAM: Jurnal Sosial Dan Budaya Syar-I*, 6(2), 155–178.
<https://doi.org/10.15408/sjsbs.v6i2.11041>
- Hiariej, E. O. . (2009). *Pengantar Hukum Pidana Internasional*. Jakarta: Erlangga.
- Hidayat, F. (2016, December). Kapolri: Ada terorisme siber, rekrutmen & pelatihan bom lewat online. *Merdeka.Com*.
- Jacob, H. K. (2017). Peranan Penyidik Dalam Tindak Pidana Cybercrime. *VI*(6), 124–131.
- Jacob, H. K. (2017). Peranan Penyidik Dalam Tindak Pidana Cybercrime. *VI*(6), 124–131.
- Kadir, N. K., Judhariksawan, J., & Maskun, M. (2019). Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes. *Fiat Justisia*, 13(4), 333.
<https://doi.org/10.25041/fiatjustisia.v13no4.1735>
- Kaligis, O. C. (2012). Penerapan Undang-Undang nomor 11 tahun 2008 tentang Informasi dan transaksi elektronik dalam prakteknya. *Yarsif Watampone*.
- M. Naufal, M., & Jannah, H. (2012). Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif Dan Hukum Islam. *Al-Mawarid Journal of Islamic Law*, 12(1), 69–84.
- Malthaner, S. (2017). Radicalization: The Evolution of an Analytical Paradigm. *European Journal of Sociology*, 58(3), 369–401.
<https://doi.org/doi:10.1017/S0003975617000182>
- Marpaung, E. L., Astuti, M., & Ibrahim, A. (2017). Analisis Cyber Law dalam Pemberantasan Cyber Terorism di Indonesia. *Annual Research Seminar 2017*, 3(1), 17–21.
- Nadjib, M., & Cangara, H. (2017). Cyber terrorism handling in Indonesia. *The Business and Management Review*, 9(2), 274.
- Naro, W., Syatar, A., Amiruddin, M. M., Haq, I., Abubakar, A., & Risal, C. (2020). Shariah Assessment Toward the Prosecution of Cybercrime in Indonesia. *International Journal of Criminology and Sociology*, 9(1), 572–586.

- Nasrullah, R. (2012). Media Baru dan Potensi Terorisme Virtual. *EMPATI: Jurnal Ilmu Kesejahteraan Sosial*, 1(1), 59–70. <https://doi.org/10.15408/empati.v1i1.9768>
- Neely, P. R. & M. T. A. (2018). Policing Cyber Terrorism. *Journal of Cybersecurity Research*, 3(1), 13–19. <https://doi.org/10.19030/jcr.v3i1.10227>
- Nurul, R. E. S., Fitriati, F., & Rianda, S. (2020). Pengaturan Terhadap Cyber Terrorism Dalam Hukum Pidana Indonesia. Universitas Bung Hatta.
- Priyambodo. (2006, September). Indonesia Pertama Kali Bongkar Kasus "Cyber-Terrorism." *AntaraNews.Com*.
- Putra, B. P. (2020). Fenomena Cyber-terrorism di Indonesia: Penanggulangan Website Radikal dan Kaitannya dengan Demokrasi Pancasila. *Kompas.Com*. <https://www.kompasiana.com/bimosenopratamaputra/5e202a04d541df23d404c372/fenomena-cyber-terrorism-di-indonesia-penanggulangan-website-radikal-dan-kaitannya-dengan-demokrasi-pancasila>
- Putri, S. D. (2019). Cyber Terrorism; Strategi Propaganda dan Rekrumen ISIS di Internet dan Dampaknya Bagi Indonesia Tahun 2014-2019. *Journal of International Relations*, 5(4), 827–833.
- Putri, S. D., & Wahyudi, F. E. (2019). Cyber Terrorism: Strategi Propaganda dan Rekrutmen ISIS di Internet Dan Dampaknya Bagi Indonesia Tahun 2014-2019. *Journal of International Relations*, 5(4), 827–833.
- Rachman, F. (2018). Islam dan Terorisme. *Islam Futura*, VII(2), 49–59. <https://doi.org/10.22373/jiif.v7i2.3064>
- Rahman, A. (2018). Memahami Jihad Dalam Perspektif Islam (Upaya Menangkal Tuduhan Terorisme Dalam Islam). *J-PAI: Jurnal Pendidikan Agama Islam*, 4(2), 141–158. <https://doi.org/10.18860/jpai.v4i2.5427>
- Ramadhan, I. (2019). Strategi Keamanan Cyber Security di Kawasan Asia Tenggara; Self-Help atau Multilateralism? *Asia Pacific Studies*, 3(2), 181–192. <https://doi.org/10.33541/japs.v3i1.1081>
- Rochmawati, I. (2016). Cyber Terorisme Dan Eksistensi Gerakan Terorisme Kelompok Islam Radikal Di Indonesia. *INOVATIF: Jurnal Penelitian Pendidikan, Agama Dan Kebudayaan*, 2(1), 33–53.
- Rustam, S. (2016). Pembontakan terhadap pemerintahan yang sah (bugah) dalam perspektif hukum Islam. *Ijtihad: Jurnal Wacana Hukum Islam Dan Kemanusiaan*, 16(1), 67–83. <https://doi.org/10.18326/ijtihad.v16i1.67-83>
- Sampath Kumar Venkatachary, J. P. & R. S. (2018). Cybersecurity and cyber terrorism- in energy sector – a review. *Journal of Cyber Security Technology*, 2(3–4), 111–130. <https://doi.org/10.1080/23742917.2018.1518057>
- Sari, B. D. A. C. (2017). Media literasi dalam kontra propaganda radikalisme dan terorisme melalui media internet. *Peperangan Asimetrik*, 3(1), 15–31.
- Siagian, B. D. O., & Sumari, A. D. W. (2015). Radicalism Discourse Analysis on Online Sites in Indonesia. *Jurnal Pertahanan*, 1(2), 67–92. <https://doi.org/10.33172/jp.v1i2.57>
- Susanto, N. H. (2018). Menangkal Radikalisme Atas Nama Agama Melalui Pendidikan Islam Substantif. *Nadwa: Jurnal Pendidikan Islam*, 12(1), 65–88. <https://doi.org/10.21580/nw.2018.12.1.2151>
- Wajdi, M. B. N. (2017). Islam dan Radikalisme (Mengurai Makna Terorisme). *OSF Preprints*, Nopember, 1–7. <https://doi.org/10.31219/osf.io/rn69g>
- Wibowo, P., & Hapsari, D. (2020). Ancaman Terorisme Islamic State of Iraq and Syria (Isis) Pasca Fase " Khilafah ." *12(1)*, 23–42.

Book

- 'Audah, A.Q. (2013). *al-Tasyri' al-Jina'i al-Islami; Muqaranan bi al-Qanun al-Wadh'i*, Jil. II (II). Kairo: Maktabah al-Taufiqiyah.
- Al-Buti, M. S. R. (n.d.). *Muhadharat fi Fiqh al-Muqaran*. Damaskus: Dar al-Fikr.
- Arake, L. (2013). *Islam Melawan Kekerasan dan Terorisme* (1st ed.). Yogyakarta: Prudent Media.
- Hiariej, E. O. . (2009). *Pengantar Hukum Pidana Internasional*. Jakarta: Erlangga.
- Sitompul, J. (2012). *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana*. Tatanusa.
- Syatar, A., & Abubakar, A. (2020). *Filosofi 'Uqubah Islamiyah Versi Ramadhan Al-Buti; Relevansi dengan Pemidanaan dalam Sistem Hukum Indonesia*. Gowa: Alauddin University Press

Disertation

- Nurul, R. E. S., Fitriati, F., & Rianda, S. (2020). Pengaturan Terhadap Cyber Terrorism Dalam Hukum Pidana Indonesia. Universitas Bung Hatta

Website

- Hidayat, F. (2016, December). Kapolri: Ada terorisme siber, rekrutmen & pelatihan bom lewat online. *Merdeka.Com*.
- Priyambodo. (2006, September). Indonesia Pertama Kali Bongkar Kasus "Cyber-Terrorism." *AntaraNews.Com*.
- Setyawan, F. A. (2019, October 23). Menag Fachrul Razi: Saya Bukan Hanya Menteri Agama Islam Saja. *CNN Indonesia*. <https://www.cnnindonesia.com/nasional/20191023195949-20-442314/menag-fachrul-razi-saya-bukan-hanya-menteri-agama-islam-saja>
- Sugihartati, R. (2020, May). Ancaman Cyber Crime di Tengah Wabah Covid-19. *Media Indonesia*.
- Yusuf, O. (2017, May). Rumah Sakit Indonesia Jadi Korban "Terorisme Cyber." *Kompas.Com*.

Received on 19-05-2021

Accepted on 06-07-2021

Published on 03-08-2021

<https://doi.org/10.6000/1929-4409.2021.10.146>

© 2021 Bakry et al.; Licensee Lifescience Global.

This is an open access article licensed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted, non-commercial use, distribution and reproduction in any medium, provided the work is properly cited.