JURNAL MEDIA HUKUM
Vol. 27, No. 2, December 2020
P-ISSN: 0854-8919, E-ISSN: 2503-1023
Nationally Accredited Journal, Decree of MoHE No. 148/M/KPT/2020.

Cyberterrorism and its Prevention in Indonesia

Dian Alan Setiawan
Faculty of Law, Universitas Islam Bandung, Indonesia
E-mail: dianalan.setia@yahoo.com

ARTICLE INFO

Keywords:
prevention, cybercrime, cyberterrorism

How to cite:
Setiawan, D. A. (2020). Cyberterrorism and its Prevention in Indonesia. Jurnal Media Hukum, 27(2), 256–272

Article History:
Received: 01-07-2020
Reviewed: 21-08-2020
Revised: 24-08-2020
Accepted: 31-12-2020

ABSTRACT

In cyberspace, cyber technology gives rise to illegal activities that are legally referred to as cybercrimes. Cybercrime appears in various forms including cyberterrorism. The purpose of this research is to discuss the development of cyberterrorism and to explore the efforts made by the Government in addressing and controlling cyberterrorism in Indonesia. This normative legal research examines the application of the relevant legislation, especially Law No. 19 of 2016 on the Amendment to Law No. 11 of 2008 on Information and Electronic Transactions and Law No. 5 Year 2018 on the Amendment of the Law No. 15 Year 2003 on the Eradication of Crime of Terrorism. It is found that the act of cyberterrorism can be prevented through both technological and legal approaches.

DOI: 10.18196/jmh.20200156

1. Introduction

In the past 20 years, Criminals have been resorted to the acts of robberies, abductions, car stealing, donations of shares, DVD piracy, and free piracy loans. All of these methods will soon end with the developing cyber technology. Some experts say that this type will become obsolete because it is present in the advancement of Cyber technology. Many aircraft will use fly by wire controls so it makes more sense for criminals to pass hacking into the navigation system and to divert the direction of the plane as wish. The progress of cyberspace science and technology is a necessity in a century of increasingly advanced human civilization.[1]

Virtual world technology that is connected with many internet networks has a new phenomenon in human interaction in cyberspace. Cyber technology is the use of the internet as a medium for unlimited communication and interaction which then has a negative impact because of the emergence of media through Cyber which is commonly

[1] Darlis, A. (2017). *Cyber Narcoterrorism*. Kompasiana. https://www.kompasiana.com/andidarlis/590add24b67e61c3109174d6/cyber- (Accessed on February 17, 2020)

known as Cybercrime. The irresponsible use of cyber technology may amount to a criminal conduct which can potentially pose as threats to the country. The types and violations of Cybercrime vary greatly Including the act of electronic eavesdropping, electronic data theft, online dissemination of pornography, increased illegal funds, handling via the internet, internet gambling, vandalism sites, deletion of damaging systems through viruses, trojans, signal bases and the like appear in shape like that.

The use of "Cyber" for crimes committed by parties who have high ability and expertise in computer science, Cybercrime's agreement on computer mastery and computer programming to make malware scripts/codes, they can analyze the workings of computer systems and networks, and are able to find a solution for the system will then use this weakness to get into preventative measures such as safekeeping. Cyber is currently also used to launch terror (cyber terrorism). Indoctrination/dogma through Cyber which is able to produce many people for jihad as well as recruitment which is guided by ISIS network to come to Syria to provide forms through Cyber media. Propaganda techniques will cause fear and illegal fundraising are methods to get funds for terrorist purposes. The Coordinating Minister for Political, Legal and Security Affairs Wiranto said, the formation of the National Cyber Agency began with the government's request to compile acts of terrorism in cyberspace or cyber terrorism. According to Wiranto, discussions on cyber terrorism have become an international concern. Meanwhile, Indonesia itself does not yet have a single body that can protect cyber activities nationally. In an international meeting on anti terrorism in August 2016 in Bali, 36 countries discussed various things that could be resolved to deal with the rapid development of terrorism. Wiranto said that currently the protection of terrorism in various countries is focused on the protection of cyberspace. Many countries already have cybersecurity services that handle financing and communication between terrorist groups. Their communication, how to train and assemble bombs carry out financial transactions all through cyberspace. Other countries are already so advanced to place cyberspace as the main activity in their country[2].

In addition, Wiranto will also prepare a National Cyber agent that will not require a large fee. Because, the government will again empower the State Code Institute to become the forerunner of the National Siberian Agency. Once established, the National Cyber Agency will also protect the flow of cyber traffic, especially in the fields of e-commerce, banking, and discuss the importance of finance. In addition, the National Cyber Agency will also coordinate cyber defense bodies at the Ministry of Defense, cyber intelligence at the National Intelligence Agency (BIN), and cyber crime units at the Indonesian National Police (Polri).

At this time, the crime of Cyber Terrorism has risen to become Cyber Narcoterrorism, so that it has become one of the potential forms of crime in the future. At this time, the crime of Cyber Terrorism has increased to become Cyber Narcoterrorism so that it has become one of the potential forms of crime in the future that can threaten the stability of a country. Cyber Narcoterorism is a new phrase in the Cyber world that needs to be watched out by the Indonesian security authorities. Cyber Narcoterrorism is a term conveyed by TNI Commander General TNI Gatot Nurmantyo and calls on all ranks of

[2] Erdianto, K. (2017). C*yberterrorism Salah Satu Alasan Dibentuknya Badan Siber Nasional*. *Kompas.com*, nasional.kompas.com/read/2017/01/09/19163671/.cyber.terrorism.salah.satu.alasan.dibentuknya.badan.siber.nasional. (Accessed on February 13, 2020)

the TNI, Territorial Command and Intelligence apparatus to be aware of this threat. Cyber Narcoterorism is a new type of crime in cyberspace but has a broad impact on the security and national sovereignty of a nation. Cyber Narcoterrorism can be interpreted as efforts, work, activities and actions carried out by certain parties/ groups both state and non-state actors circulating narcotics for the purpose of financing terrorist activities through the use of cyber media. This definition is a platform of understanding that is used as a guide for the TNI in observing the development of Cyber Narcoterrorism.

Seeing the number of Cyber media users, concrete anticipation steps are needed so that the potential to become victims or Cyber Narcoterrorism actors can be minimized. Even if necessary, Indonesia must have a special independent institution as a supervisor and to provide recommendations for legal action for this cybercrime. As a concrete step that can be taken to reduce Cyber Narcoterrorism such as: Recruiting IT experts to strengthen IT within the TNI, Strengthen and improve the quality of knowledge and skills of personnel serving in the Complex by providing continuous IT education and training, Procurement electronic communication infrastructure, in collaboration with law enforcement officials in tackling cyber narcoterrorism, and compiling software and most importantly, Indonesian Army should be an example in using social media, filling in good and true content. The massive use of social media by many groups must be a serious concern and have the ability to fortify the negative influence of the use of social media by groups who are not responsible for society. The minimum effort that can be done for the current condition is filtering/blocking as an initial counterintelligence action to deal with the threat of Cyberterrorism. The era of globalization which no longer recognizes state boundaries, Cyberterrorism is one of the models of war without troops. At present, Indonesia is a fertile ground for the cadre of terrorism and a safe place to shelter for terrorist activities[3].

The interaction between the use of information technology and human motives to commit terrorism in cyberspace or in the virtual world gives a new understanding of terrorism, namely cyberterrorism. In some cases, the development of these technologies is used by radical groups to launch their activities[4].

Based on this, the problem is:

a. What is the new form of cyberterrorism crimes committed by terrorists by making the internet a media or target of attacks?

b. What are the efforts made in the prevention of cyberterrorism in Indonesia?

The expected benefits are to provide general input for the development of law, specifically in the field of specific criminal law (criminal acts outside the Criminal Code) relating to (cybercrime). Practically, it is expected to provide input to the government in the context of policy making and the formation of legislation related to cybercrime, especially relating to terrorism and as information material to the public regarding cyberterrorism crimes.

---

[3] Atmasasmita, R. (2011). *Laporan Akhir Naskah Akademik RUU No. 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme*. phn.go.id/data/documents/naskah_akademik_ruu_tentang_pemberantasan_tindak_pidana_terorisme.pdf (Accessed on February 25, 2020)

[4] Salam, M. F. (2005). *Motivasi Tindakan Terorisme* (1st ed.). Mandar Maju. p. 216.

This research aims to understand that crime is still relatively new, minimizing terrorist groups' ability to attack information networks and electronic transactions as a tool to spread terror widely. Therefore, this study briefly describes cyberterrorism. It is also necessary to think about controlling to prevent the development of cyberterrorism in the future.

2. Method

The research method used in this study is a normative research method, namely research that is focused on examining the application of the rules or norms in positive law[5]. Normative research is legal research carried out by examining library materials or secondary data as a basis for research by conducting a search of regulations and literature relating to the issue under study[6]**.** The author uses the statutory approach and conceptual approach[7], while the data collection method in this research through library research by searching the legal principles, statutory regulations and other documents that related to the problem under study[8].

3. Analysis and Results

3.1. Development of Cyber Terrorism Crimes Committed by Terrorists by Making the Internet a Media or Target of Attacks

The development of the globalization era that gave rise to the Internet media has made the communication media used by terrorists increasingly develop. They try to adapt their abilities to the development of existing communication and information technology. The transformation from the use of conventional media to new media, namely the Internet which gave rise to the phenomenon of cyber-terrorism moreover it would use artificial intelligence technology as well[9]. Cyber-terrorism has become a world issue that requires all countries to be able to dominate the world of the Internet to find out terrorist acts. The more rapid development of new media technology, the more sophisticated the media used by terrorists and the greater the acts of terrorism. The benefits of advancing information and communication technology especially the internet have touched all sides of modern human life. This positive side was apparently followed by the dark side of internet use[10]. The internet has evolved, which was originally used for military purposes and has become a target for scientific and criminal means. Internet users are not only general users but are used by spies and terrorists. After September 11, 2001 attacks on New York and the Pentagon, terrorism received much attention from all over the world. The world community hopes to predict the next act of terrorism because everyone believes that terrorism will happen.

---

[5] Ibrahim, J. (2012). *Teori dan Metodologi Penelitian Hukum Normatif*. Bayumedia Publishing. p.25.

[6] Soekanto, S., & Madmuji, S. (2015). *Penelitian Hukum Normatif : Suatu Tinjauan Singkat*. PT RajaGrafindo Persada. p. 49.

[7] Marzuki, P. M. (2010). *Penelitian Hukum* (Cet.6). Kencana Prenada Media Group. p.35.

[8] Ibid.,

[9] Rahman, R. A., & Habibulah, R. (2019). The Criminal Liability of Artificial Intelligence: Is It Plausible To Hitherto Indonesian Criminal System? *Legality : Jurnal Ilmiah Hukum*, 27(2), 147. https://doi.org/10.22219/jihl.v27i2.10153. P. 148-149

[10] Trisa, U. (2014). Kebijakan Anstisipatif Hukum Pidana Untuk Penanggulangan Cyberterrorism. *Masalah-Masalah Hukum*, 43, 1–10. https://media.neliti.com/media/publications/158219-ID-none.pdf)

One factor that can predict their actions is what method they use to send their terror to the targeted population[11]. This media is related to terrorism as their communication tool.

Seeing the great dependence on the internet, terrorist attacks aimed at him pose a serious threat which includes a new territory for national security and public policy. Therefore, a country must start thinking about securing its network system from attacks, especially from cyberterrorism. So it is very important that the phenomenon of cyberterrorism is must be well understood because of the shadow of terrorist attacks that always lurk all of us all the time. Media and terrorism are two central themes that attract attention because they have a common thread. The common thread between media and terrorism is inseparable from the aspect of news commercialization. Terrorism is a social fact that can be exploited in the interest of increasing news consumption. Meanwhile, modern terrorism utilizes communication media to affect the public through a form of terror propaganda. There is a symbiotic relationship between the two who meet at the point of interest in information needs and the desire to be covered by the media[12].

The connection between terrorists and the media was also revealed by Hendropriyono that there are mutually beneficial conditions (symbiotic mutualism) between terrorists and the media. The media has strengthened terrorist acts as politically important out of proportion[13]. Terrorism is the deliberate use or threat of using violence against civil society or against civil society targets to defend political objectives. The terrorism side is based on three important elements, namely[14]:

a. The essence of the act of terrorism in the use of threats or violence. Based on this, element an activity that does not include violence or the threat of violence will not be defined as terrorism (including non-violent protests, peace demonstrations, tax rebellions, and the like).
b. The purpose of terrorism is always political. The aim is to defend political goals, change the regime, change people with power, change social or economic policies. In the absence of political goals, an action cannot be defined as terrorism. An act of violence against civil society that has no political, criminal or criminal purpose is not related to terrorism. Some experts put the ideological or religious goals on the list of goals that are political in nature.
c. The target of terrorism is civil society. Terrorism exploits the fragility of civil society to cause intense anxiety and and provokes intense media reaction by attacking against civil society targets.

In its development, technological advancements and the era of globalization gave rise to new media that allowed terrorists to attack in ways previously unimaginable

[11] Susan W Brenner, "Cyber-terrorism: How real is the Threat?," *Media Asia*, last modified 2001, https://www.tandfonline.com/doi/abs/10.1080/01296612.2002.11726680. (Accessed on March 7, 2020)
[12] Sukarno & Adam W, "Dilema Peliputan Terorisme dan Pergeseran Pola Framing Berita Terorisme di Media Massa," *Jurnal Ilmu Sosial dan Ilmu Politik,* 14 (3) (2011). p. 333–348.
[13] A.M Hendropriyono, *Terorisme: Fundamentalis Kristen, Yahudi, Islam* (Jakarta: PT Kompas Media Nusantara, 2009). p. 47.
[14] Boaz. Ganor, "Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter?," *Police Practice and Research: An International Journal*, last modified 2002, https://www.ict.org.il/Article/1123/Defining-Terrorism-Is-One-Mans-Terrorist-Another-Mans-Freedom-Fighter#gsc.tab=0. (Accessed on March 20, 2020)

through the Internet. Acts of terrorism that are unexpected and capable without leaving a trace. And, acts of terrorism that are not limited by time and affordability of place.

The roots of the development of cyberterrorism can be traced since the early 1990s, when the growth of the Internet was growing rapidly and the emergence of the information community. In the United States since then a study was conducted on the potential risks that would be faced by the United States over its dependence on networks and high technology. The dependence of the United States is so high on networks and technology that one day America will face what is called "Electronic Pearl Harbor." Psychological, political, and economic factors are a combination that makes the American fear increases on the issue related to cyberterrorism. In 1999, President Clinton came up with a budget proposal to deal with cyber terrorism in the amount of $ 2.8 billion, which was also intended for handling national security from the threat of internet dangers.

This fear is quite reasonable, because there were several incidents categorized as cyberterrorism, including in April and March 2002, in the United States, precisely the state of California, there was a total loss of electricity supply caused by crackers from China which infiltrated the power network generator in the region. Another example is the action of 40 crackers from 23 countries joining the Israeli-Palestinian cyber war between October 2000 and January 2001. A group calling itself UNITY and having links to the Hezbollah organization planned to attack the Israeli government's official website, financial and banking system, ISPs Israel and attacking the e-commerce sites of the Israeli Zionists.

The shift from conventional terrorism to cyberterrorism is due to several factors. Weimann in his article "How Modern Terrorism Uses the Internet" tells eight reasons why a shift in the area of terrorism activities from conventional to cyberterrorism is as follows[15]:

a. Ease of access. Cyberterrorism can be done remotely. This means that cyberterrorism can be carried out anywhere through remote control.
b. At least the regulations, censorship, and all forms of government control.
c. The potential for globalizing information dissemination.
d. Anonymity in communication. This is common in the world of the Internet. Most people interact on the Internet using a fake name or nickname
e. Fast information flow.
f. Low cost to develop and maintain a website, besides that in carrying out cyberterrorism that is needed, generally only a computer device that is connected to the Internet network.
g. Multimedia environment that makes it easy to convey the intent and purpose of terror.
h. Better ability than traditional mass media in presenting information.

[15] Weimann, G, "*How Modern Terrorism Uses the Internet*", United Space Institute of Peace: Special Report, https://www.usip.org/sites/default/files/sr116.pdf (Accessed on April 8, 2020)

To explore what and how cyberterrorism, it is necessary to first give a definition of the cyberterrorism. Some institutions and experts provide definitions related to cyberterrorism. The first definition is obtained from the Black's Law Dictionary, which explains the following: Cyberterrorism. Terrorism committed by using a computer to make unlawful attacks and threats of attack computers, networks, and electronically stored information, and actually causes the target to fear or experience harm. Terrorism is carried out by using computers to carry out attacks on computers, computer networks, and electronic data that causes fear of victims. From this definition, the main elements of cyberterrorism can be seen, namely:

a. computer use,
b. the aim is to carry out attacks, these attacks are aimed at computer systems and data,
c. and the result of fear of the victim.

The next definition issued by the Federal Bureau of Investigation (FBI) states as follows[16]: cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents. (Can be freely translated as, cyberterrorism is a planned attack with political motives on information, computer systems, and data that results in violence against civilians and is carried out by sub-national groups or secret groups).

The next definition is given by Dorothy Denning, which is: Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in to furtherance political or social objectives (cyberterrorism is the convergence of cyberspace and terrorism). This definition refers to acts against the law by attacking and threatening to carry out attacks on computers, networks and information stored therein for the purpose of intimidating or coercing the government or society for political or social purposes).

The Internet and Terrorism, Lewis states as follows[17]: The Internet enables global terrorism in several ways. It is an organizational tool, and provides a basis for planning, command, control, communication among diffuse groups with little hierarchy or infrastructure. It is a tool for gathering intelligence, providing access to a broad range of materials on potential targets, from simple maps to aerial photographs. One of its most valuable uses is for propaganda, to relay the messages, images and ideas that motivate the terrorist groups. Terrorist groups can use websites, email and chatrooms for fundraising by soliciting donations from supporters and by engaging in cybercrime (chiefly fraud or the theft of financial data, such as credit card numbers).

Based on this statement, we know the possibility or other forms of cyberterrorism, namely the use of information technology, in this case the Internet as an organizational tool that functions as a tool for planning, giving commands, communicating between

[16] Overview of Cyber-Terrorism," last modified 2002, www.cybercrimes.net/Terrorism/overview/page1.html. (Accessed on April 9, 2020)
[17] James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* (Center for Strategic and International Studies (CSIS), 2002). p.41

group members[18]. In addition, the information technology base becomes an important part of terrorism, namely as a propaganda media for terrorist activities. In its development, technological advancements and the era of globalization gave rise to new media that allowed terrorists to attack in ways previously unimaginable through the Internet. Acts of terrorism that are unexpected and capable without leaving a trace. Acts of terrorism that are not limited by time and affordability of place. The use of Internet-based media shows that terrorists understand the media as a strategy and tactic tool in their terrorist activities. The use of the Internet by terrorists in various forms of messages, both audio-visual, image, and words simultaneously, and continuously aims to make the world community remain aware of the existence of terrorists. Global terrorism uses various types of new media in several ways to generate publicity and attract public attention[19]. The variety of media used is adjusted to the target audience they want to communicate[20].

Al-Qaeda figures who are very active in using Internet applications in their terrorist activities are Al-Awlaki, who was born in New Mexico and got his degree from the University of Colorado and the University of San Diego[21]. The use of Internet media is very clearly used for websites, YouTube, social media and, online magazines. Plus, online games are added by intelligence as well as the media they coordinate in developing strategies. The variety of online media applications is used maximally by terrorists for their activities.

3.2. Efforts to Control the Development of Cyberterrorism

Cyberterrorism is a form of crime that is difficult to conduct surveillance and is also a crime that is cross-country in nature so that it sometimes adds complexity in terms of prosecution. This type of crime is also classified as a criminal offense between different legal systems, which in turn impacts the danger of this crime picture. Therefore, the discussion in this section examines more about a technological approach that is useful as a control of cyberterrorism and a legal approach to dealing with cyberterrorism. The goal is that efforts to prevent the development of cyberterrorism into a measured and systematic response as part of a rational policy to anticipate cyberterrorism. When viewed from the scale of action and its organization, terrorism is distinguished between national terrorism, international terrorism, and transnational terrorism. The National network of organizations and acts of terrorism are limited to certain countries' territories. The threat of cyberterrorism can afflict all countries, including Indonesia. The use of internet facilities to carry out terrorism needs to be watched out for its movements given that almost vital state-owned facilities, public facilities, and community activities are currently utilizing the internet and are dependent on the internet because of the speed and flexibility that can connect them all. Cyberterrorism attacks that attack anything that is connected to the internet, especially vital objects

[18] Gunawan Y., Aulawi M. H., Ramadhan A. R., (2020), Command Responsibility of Autonomous Weapons Systems under International Humanitarian Law, *Jurnal Cita Hukum*, Vol. 7 No. 3 (2019), pp.351-368, DOI: 10.15408/jch.v7i3.117255.

[19] *Terrorist groups recruiting through social media., CBC News*, 2012, http://www.cbc.ca/news/technology/terrorist-groups-recruiting-through-social- media-1.1131053 (Accessed on April 17, 2020)

[20] Lumbaca, S.,& Gray, D. . (2011). The Media As An Enabler For Acts Of Terrorism. *Global Security Studies*, 2 (1). p. 53

[21] D.M Seib, P. & Janbek, *Global Terrorism and New Media: The post-Al Qaeda generation.* (New York: New York: Routledge Taylor & Francis Group, 2011). p. 35.

belonging to the government that can interfere with their functions, can even make a greater victim than conventional terrorism.

Meanwhile, international terrorism, directed at foreigners and foreign assets, is organized by governments or organizations of more than one country, and aims to influence the policies of foreign governments. Transnational terrorism is global network terrorism that prepares a global revolution for new world order (part of international terrorism that is becoming radical)[22]. This is a picture of the development of the world of terrorism crime, which is increasingly becoming more systematic and organized.

It has been stated above that there are two approaches related to preventing the development of cyberterrorism, these are as follows:

a. Technological Approach

Cyberterrorism is a type of crime that is closely related to terrorists who use advanced technology as a means or target of attacks. So the most rational effort in dealing with new variants of crime is to prioritize a technological approach (techno prevention). One of the problems that become a problem in cyberterrorism crime is a matter of determining one's legal identity. Legal identity (legal identity) is often disguised, falsified, or stolen in the cyber world. By using the data themselves disguised as a terrorist can access the network, data to launch the action. To solve the problem of misusing one's personal data to carry out terror attacks, the anticipatory way that can be used is to activate biometrics technology[23]**.** The basic logic used in this technology is the application of technology to control and restrict internet access. Biometric systems consist of two processes: registration (matching) and matching (matching). At the registration stage, for the first time, individual characteristics must include fingerprints. Images obtained in general can be converted into a template. In the matching phase (matching) of biometrics that describe the characteristics of the individual was adjusted to the live template by comparing the previous data whether it is suitable or not. The key word for the operation of the biometric system in the verification method is "are you who you claim to be?". In addition to the above, it is necessary to have an antidote to cyberterrorism, such tools include:

1) SAT (Security Administrator's Tool for Network Analysis), the equipment needed to do a complete and complete analysis of a computer network system so that the performance as well as the weak points of the computer network can be identified.
2) TCP Wrapper to monitor the network in a computer (trafficking), especially in the case of data packet traffic in a network that uses a TCP / IP protocol (internet protocol) so that data packets that pass through can be monitored properly.
3) Crack to do password security testing where the benefits are to find out the weaknesses of the user's passwords, because not all users know how to create a secure password. Some even do not use it at all.
4) Firewall, is a protection system to carry out monitoring of data packet traffic that goes to or leaves a computer network. So that the data packet that has been

[22] Ali, M. (2012). *Hukum Pidana Terorisme Teori dan Praktik*. Gramata Publishing. p. 10.
[23] Trisa, U.,*Op.Cit.*

checked can be accepted or rejected and even modified before entering or leaving the network.

b. Legal Approach

Criminal Code (KUHP) and Criminal Procedure Code (KUHAP) in Indonesia are based on regulations, laws, and regulations applied by the police, prosecutors, and courts at all levels. Court institutions that process court proceedings, from education to court decisions in court. However, lately, through the development of the times, especially technology in this paper, we can find different litigation with the Criminal Procedure CodeIn other existing regulations, special regulations (*lex speicialis*) of the provisions of the law include criminal justice. One critical law to be observed and discussed is Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 on Information and Electronic Transactions. [24].

One of the characteristics of cyberterrorism is that it crosses national borders. The problem then is that a country's law must be oriented to how to make harmonization efforts. The goal is so that a country's legal system does not overlap either within the country's internal affairs

1) Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Electronic Information and Transactions (Undang-Undang No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Elektronik**)**

It is a law that regulates technology-based crimes (cyber crime), while cyberterrorism is a part/type of cybercrime. Criminal provisions in the Information and Electronic Transactions are contained in Chapters XI Articles 45 through 52. The following are the formulation of several articles in Chapter XI regarding criminal provisions. Based on the provisions of the articles in Chapter XI regarding criminal provisions in the ITE Law, it can be identified several acts that are prohibited (elements of a criminal offense) that are closely related to criminal acts of cyberterrorism in each of the articles. **Article 30** Concerning cyberterrorism in the form of unauthorized access to computer systems and services. some examples in Article 30, namely[25]:

a) Data Mining

The internet is a huge source of information and anyone can exploit it and terrorists can use it too. The Internet allows access to highly detailed and accurate maps, schemes and other data sources, allowing terrorists to collect this information as a very potential target. More importantly, once this data has been collected, it is compiled into one 'volume' and into a 'how' and as a manual distributed among terrorist organizations.

b) Publicity and Propaganda

As stated by terrorism researcher Dr. Maura Conway states that 'Every machine connected to the Internet has the potential to be a printer, broadcast station or

[24] Satria, H. (2018). Restorative Justice : Paradigma Baru Peradilan Pidana. *Jurnal Media Hukum*, 25(1), 111-123.. https://doi.org/0.18196/jmh.2018.0107.111-123 (Accessed on April 10, 2020)

[25] Mantra, I. (2010). *7 Ancaman Teroris Lewat Internet*. Detiknet. http://www.ignmantra.id/2010/05/ (Accessed on April 26, 2020)

forum. The Internet is a suite of un-parallel media. Terrorists no longer have to own these messages, let alone edit them by the media. On the other hand, they (terrorists) can quickly spread the information they choose or want and send to anywhere in the world. Terrorists do select and distribute information on their actions even though their actions can be said to be unusual.

c) Recruitment

In this section basically related to propaganda, terrorist organizations can monitor users who browse their web, capture their profile and information about them and if it is considered it may be very useful to recruit them and contact them. The recruitment process begins when internet users start absorbing propaganda on websites that they frequently visit and that are of interest to them.

Article 31 is related to Hacking crime. this law is related to cyberterrorism in the form of cyber sabotage and extortion. some examples in article 32, namely[26]:

a) Funding

Terrorist groups have made full use of the internet's capabilities to create funds, whether those funds are legitimate or otherwise. The main method for terrorists to achieve this is by:

(1). Selling goods, items directly related to a terrorist organization such as CDs, DVDs and books of that organization.

(2). Appeal-based websites and e-mails, i.e. sending email to registered investigators interested in the group's website, posting messages on newsgroups / forums and their websites that will provide directions, how and where the donation can be obtained.

(3). Deception, using seemingly legitimate charities or businesses whose donors are not aware of and then directing the funds to terrorist activities.

(4). Criminal activity, namely carrying out illegal/criminal activities to raise funds for these terrorist groups, including credit card fraud, online brokers, and online gambling.

b) Communications and Networking

Terrorist groups have recently changed and have a clear hierarchy in the organization with a designated leader, have multiple leaders and independent leader cells, so that their leader can hide in safety. The Internet facilitates communication between cells allowing manual and information exchange. The internet also helps internal communication within cells, especially in relation to attack planning. To avoid being detected and targeted by security forces, messages are often sent by groups via very popular e-mails, such as Hotmail and Yahoo and can also be sent from public places such as libraries and internet cafes, sometimes also using chat-rooms to facilitate their activities. In addition, steganography can be used to hide information embedded in graphic files on one of these websites. Graphic files can also be used to send very subtle messages such as reversing the orientation of a graphic gun, which means it can plan the

[26] *Ibid.*,

next phase and continuation of an operation. In order to communicate, one of the terrorists creates a web-based e-mail (webmail) instead of sending it but saves it as an online draft. The recipient then 'logs in' to this account, reads it and, then deletes all these messages. The next day, a new account is created and used as before and, so on, it not is very difficult to trace the user (user account).

Article 33 concerns cyberterrorism in the form of unauthorized access to computer systems and services. Some examples in Article 33, namely[27]: The use of disinformation by terrorist groups is often used to arouse fear and panic in others by sending various threats to their victims such as viewing videos of brutal executions, creating psychological attacks etc,. through the use of cyberterrorism threats. Disinformation can also be used to distract from backlash by releasing various hoax attacks that make it difficult for the government and law enforcement officials to track them down. However, these measures are not completely effective due to the layered nature of the current security system for example, after receiving information about a potential attack (CERT Alert), the level of security across the spectrum across the country increases from black, gray and finally to white or free from threats. Cyber terrorism. Therefore, it appears that the perspective of the Information and Electronic Transaction Law is emphasizing aspects of the use/security of Electronic Information Systems or Electronic Documents, and misuse in the technology and electronic transactions carried out by cyberterrorism actors.

The act of disinformation by terrorists in the paragraph above has occurred in Indonesia, namely, the WannaCry ransomware attack has spread widely throughout the world, including Indonesia. The malicious program has even taken hostage computer systems in a number of hospitals in Jakarta, making it difficult for medical services to patients and in accessing patient data. Director General of Applications and Information at the Ministry of Communication and Information, Semuel Abrijani Pangarepan, called the ransomware attack a form of cyber terrorism. Complaints from hospitals regarding the queuing computer system for patients who have stopped working due to ransomware infection are not only hospitals in Indonesia that are victims of this malicious program because WannaCry has spread to nearly 100 countries around the world. Doctors, there have difficulty accessing patient medical records because their computers are locked. Hundreds of computers infected with WannaCry itself actually spread randomly, quickly, and widely[28].

However, some of the victims happened to come from hospitals that neglected to take precautions 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 hospitals National references 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.

---

[27] *Ibid.,*

[28] Yusuf, O. (2017). Rumah Sakit Indonesia Jadi Korban 'Terorisme Cyber. *Kompas.Com*. https://tekno.kompas.com/read/2017/05/13/17180077/rumah.sakit.indonesia.jadi.korban.terorisme.cyber.?page=all (Accessed on May 4, 2020)

Once inside, this ransomware will lock your data and computer system so that it cannot be accessed

2) Law No. 5 Year 2018 About Amendment To Law Number 15 Year 2003 Concerning The Settlement Of Substitute Government Regulations Law Number 1 Year 2002 Concerning Eradication Criminal Action Of Terrorism Becomes Law (Undang-Undang Nomor 5 Tahun 2008 Tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang)8

   Basically, the Crime of Terrorism is transnational and organized because it has peculiarities that are clandestine are secret, secretive, or underground, cross-country movements supported by the utilization of modern technology in the fields of communication, informatics, transportation, and modern weaponry, thus requiring cooperation at the international level to solve it.

   In this law, although there are not many articles that regulate crimes of terrorism in cyberspace, there are several specific articles that can be used as a reference for law enforcers in imposing sanctions on perpetrators of terrorism, especially those related to electronic means. We can see this in this Law, namely article 1 point 4 which, explains the threat of violence is every act in a manner against the law in the form of words, writings, pictures, symbols, or gestures, either with or without using any means of form electronic or non-electronic which can cause fear of people or society at large or restrain freedom intrinsic to a person or society. The words "... means in electronic form" are clearly related to technological and information means.

   Then it is confirmed again by Article 12B in this law related to information technology training carried out by terrorists both at home and abroad, dissemination of writings or documents using electronic means (information technology) as a means of recruiting and training terrorists. Therefore, it appears that the perspective of the Law on the eradication of terrorism is: provide a legal basis that further guarantees protection and certainty law in eradicating criminal acts of terrorism, as well as to meet needs and developments law in society

3) International Cooperation

   The current criminal justice system is not effective enough, facing criminals who use advanced technology that operates in the cyber world. The positive law that applies in terms of procedures, investigations, and proof (evidence) in a court hearing cannot accommodate crimes in the cyber world. Law enforcers also cannot investigate cybercrime and collect evidence properly, so that it requires technical knowledge. To improve law enforcement, a number of positive steps must be taken at the international level by educating law enforcers on the technical knowledge of information technology. This, given the global nature of cyberterrorism, the investigating institution must cooperate and have international relations so that the investigation can be carried out quickly, effectively, and appropriately. This is important because the solution to cyberterrorism can only be done at the international level and not rely only on individual countries[29]. Cyberterrorism is not

[29] Bhawan, J. (2007). *Laws on Cyber Crimes: Alongwith IT Act and Relevant Rules*. Book Enclave. p. 51

only a national problem but also an international problem. This crime has received quite extensive attention. The 8th UN Congress in Havana, the Xth Congress in Vienna, the 2005 XI congress in Bangkok, talked about The Prevention of Crime and the Treatment of Offender In addition to the efforts made by the United Nations to mobilize international cooperation to tackle cyberterrorism and find solutions to problems -problems, investigations, findings, and improvements in the way of evidence. Several organizations have come up with initiatives to create global institutions to fight cybercrime, especially cyberterrorism. The institutions such as International Services on Discovery and Recovery of Electronic and Internet Evidences, International Organization on Computer Evidence (IOCE)

4) Establishment of the National Cyber Agency

National cybersecurity is one area that needs to be encouraged and strengthened by the government as an effort to realize national security. So that the government deems it necessary to form a body by arranging the State Coding Agency to become the Census and State CODE, in order to ensure the implementation of government policies and programs in the field of cybersecurity. Based on those considerations, on May 19, 2017, President Joko Widodo (Jokowi) signed the Presidential Regulation (Perpres) No. 53 of 2017 and Amendment to Presidential Regulation No. 133 of 2017 concerning the Siber Board and the State Code. BSSN reports directly to the President. BSSN is led by a Head, assisted by a Deputy and the Main Secretariat as well as four Deputies namely, Deputy for Identification and Detection, Deputy for Protection, Deputy for Mitigation and Recovery, Deputy for Monitoring and Control. The Head of BSSN is appointed and dismissed by the President in accordance with statutory provisions. While the Deputy, Principal Secretary and Deputy are appointed and dismissed by the President at the suggestion of the Head of BSSN in accordance with statutory provisions.

4. Conclusion

The development of the globalization era that gave rise to the Internet media has made the communication media used by terrorists increasingly develop. The transformation from the use of conventional media to new media, namely the Internet which gave rise to the phenomenon of cyberterrorism. Cyberterrorism has become a world issue that requires all countries to be able to dominate the world of the Internet to find out terrorist acts. The more rapid development of new media technology, the more sophisticated the media used by terrorists and the greater the acts of terrorism that can occur. Seeing the great dependence on the internet, terrorist attacks aimed at him pose a serious threat which, includes a new territory for national security and public policy. Therefore, a country must start thinking about securing its network system from attacks, especially from cyberterrorism.

Cyberterrorism is a form of crime that is difficult to conduct surveillance and is also a crime that is cross-country in nature so that it sometimes adds to the complexity in terms of prosecution. Cyberterrorism crimes are also classified into criminal offenses between different legal systems which will have an impact on the danger of this crime picture. Therefore, the discussion in this section examines more about a technological approach that is useful as a control of cyberterrorism and a legal approach to dealing with cyberterrorism. The goal is that efforts to prevent the development of

cyberterrorism into a measured and systematic response as part of a rational policy to anticipate cyberterrorism. In this case, there are 2 approaches related to preventing the development of cyberterrorism, these are as follows, namely: 1) Technology Approach and 2) Legal Approach (Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions, Law No. 5 Year 2018 About Amendment To Law Number 15 Year 2003 Concerning The Settlement Of Substitute Government Regulations Law Number 1 Year 2002 Concerning Eradication Criminal Action Of Terrorism Becomes Law, International Cooperation, Formation of the National Cyber Agency)

References

***Books*:**

Ali, M. (2012). *Hukum Pidana Terorisme Teori dan Praktik*. Gramata Publishing.

Bhawan, J. (2007). *Laws on Cyber Crimes: Alongwith IT Act and Relevant Rules*. Book Enclave.

Hendropriyono, A. (2009). *Terorisme: Fundamentalis Kristen, Yahudi, Islam*. PT Kompas Media Nusantara.

Ibrahim, J. (2012). *Teori dan Metodologi Penelitian Hukum Normatif*. Bayumedia Publishing.

Lewis, J. A. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats: *Center for Strategic and International Studies*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

Lumbaca, S.,& Gray, D. . (2011). *The Media As An Enabler For Acts Of Terrorism*. Global Security Studies, 2 (1),.

Marzuki, P. M. (2010). *Penelitian Hukum* (Cet.6). Kencana Prenada Media Group.

Salam, M. F. (2005). *Motivasi Tindakan Terorisme* (1st ed.). Mandar Maju.

Seib, P. & Janbek, D. (2011). *Global Terrorism and New Media: The post-Al Qaeda generation.* New York: Routledge Taylor & Francis Group.

Soekanto, S. & Madmuji, S. (2015). *Penelitian Hukum Normatif : Suatu Tinjauan Singkat.* PT RajaGrafindo Persada.

Journal Articles:

Brenner, S. W. (2002). Cyber-terrorism: How real is the Threat? *Media Asia*, *29*(3), 149–154. https://www.tandfonline.com/doi/abs/10.1080/01296612.2002.11726680.

Ganor, B. (2002). Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter? *Police Practice and Research: An International Journal*. https://www.ict.org.il/Article/1123/Defining-Terrorism-Is-One-Mans-Terrorist-

Gunawan Y., Aulawi M. H., Ramadhan A. R., (2020), Command Responsibility of Autonomous Weapons Systems under International Humanitarian Law, *Jurnal*

Cita Hukum, Vol. 7 No. 3 (2019), pp.351-368, DOI: 10.15408/jch.v7i3.117255

Rahman, R. A., & Habibulah, R. (2019). the Criminal Liability of Artificial Intelligence: Is It Plausible To Hitherto Indonesian Criminal System? *Legality : Jurnal Ilmiah Hukum*, 27(2), 147. https://doi.org/10.22219/jihl.v27i2.10153

Satria, H. (2018). Restorative Justice : Paradigma Baru Peradilan Pidana. *Jurnal Media Hukum*, *25(1), 111-123*. https://doi.org/0.18196/jmh.2018.0107.111-123

Sukarno, A. W. (2011). Dilema Peliputan Terorisme dan Pergeseran Pola Framing Berita Terorisme di Media Massa. *Jurnal Ilmu Sosial Dan Ilmu Politik*, *14*(3), 333–348. https://jurnal.ugm.ac.id/jsp/article/view/10932

Trisa, U. (2014). Kebijakan Anstisipatif Hukum Pidana Untuk Penanggulangan Cyberterrorism. *Masalah-Masalah Hukum*, *43*, 1–10. https://media.neliti.com/media/publications/158219-ID-none.pdf.

Weimann G, "*How Modern Terrorism Uses the Internet*", United Space Institute of Peace : Special Report, https://www.usip.org/sites/default/files/sr116.pdf

Internet:

Atmasasmita, R. (2011). *Laporan Akhir Naskah Akademik RUU No. 15 Tahun 2003 Tentang Pemberantasan Tindak Pidana Terorisme*. phn.go.id/data/documents/naskah_akademik_ruu_tentang_pemberantasan_tindak_pidana_terorisme.pdf

CBC News. (2012). Terrorist groups recruiting through social media. *CBC News*. https://www.cbc.ca/news/technology/ terrorist-groups-recruiting-through-social- media-1.1131053

Darlis, A. (2017). *Cyber Narcoterrorism*. Kompasiana. https://www.kompasiana.com/andidarlis/590add24b67e61c3109174d6/cyber-

Kristian Erdianto, K. (2017). cyberterrorism Salah Satu Alasan Dibentuknya Badan Siber Nasional, *Kompas.com*, nasional.kompas.com/read/2017/01/09/19163671/.cyber.terrorism.salah.satu.alasan.dibentuknya.badan.siber.nasional.

Overview of Cyber-Terrorism. (2002). www.cybercrimes.net/Terrorism/overview/page1.html. (Accessed on April 9, 2020)

Mantra, I. (2010). *7 Ancaman Teroris Lewat Internet*. Detiknet. http://www.ignmantra.id/2010/05/

Yusuf, O. (2017). Rumah Sakit Indonesia Jadi Korban 'Terorisme Cyber. *Kompas.Com*. https://tekno.kompas.com/read/2017/05/13/17180077/rumah.sakit.indonesia.jadi.korban.terorisme.cyber.?page=all.

***Regulations*:**

Undang-Undang No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor

11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik ElektronikTambahan Lembaran Negara Republik Indonesia Nomor 5952)., Pub. L. No. 19 Tahun 2016 (2016).

Undang-Undang Nomor 5 Tahun 2008 Tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Und, Pub. L. No. 5 Tahun 2018 (2018).