Criminal Policy to Combating Cyberterorrism in Indonesia

Bagus Hendradi Kusuma[1]
{bagus_kusuma@mail.unnes.ac.id}

[1]LPDP Awardee, a Law Student of The Doctoral Program at Diponegoro University and Lecturer of the Faculty of Law, Universitas Negeri Semarang, Semarang, Indonesia

Abstract. Technological progress has both positive and negative impacts. The internet, as part of technological advancements, also has positive and negative impacts. The positive impact is that the internet facilitates human life in all fields, e-commerce, online banking, and various other fields. In contrast, the negative impact of the internet can trigger cybercrime. One form of cybercrime is cyber terrorism. Some say that cyber terrorism is part of a crime that uses cyber; some say that cyber terrorism is part of cybercrime. In eliminating cyber terrorism needs criminal policies in order to prevent and overcome them. Policies require to combat cyber terrorism, namely through criminal law policies or penal policies. This policy can be pursued by formulating cyber terrorism as an act that is prohibited and threatened with criminal action. While policies to prevent can be done using non-penal policies. This non-penal policy is a policy outside of criminal law. It can be done with other fields of law or social policy as crime prevention

Keywords : Criminal Policy, Criminal law, Cyber terrorism, Indonesia

1. Introduction

Technology is growing as an essential part of human life today. The development of technology in this era takes place very quickly. Also, The scope of information in the present era has unlimited space and time. The computer network which was initially only limited to the space network connected by cable, is now unlimited, because it is connected to the internet network, and can be connected to the entire world, anytime and anywhere. Internet information technology has a positive side, where internet technology makes it easy for someone to carry out activities both for communication, the world of commerce, the economy, transportation, and various other fields. Internet technology can transcend national borders so that all kinds of activities can be done immediately through the internet. Nevertheless, the development of internet technology was also followed by negative impacts other than positive impacts. The negative impact is in the form of internet abuse for a crime. The abuse of the internet for crime is known as cybercrime. Cybercrime types include cybersex/cyberporn, data diddling, carding, viruses, cybergambling, cyber defamation, cyberterrorism. The emergence of various types of cybercrime is none other than a change through the evolution of the internet's use. Initially, the use of the internet can only be done by the military. However, as time goes by, the internet can be used by all humans. Among scientists, business people, and even criminals also use the internet as part of their life activities.

Cyberterrorism is one of the negative impacts of the internet, in the form of terrorist crime through the cyber world. The dependence of human life in general at this time on the use of the internet, makes the country think about protecting the interests of human law in the internet / cyber world. The state also inevitably, when all state interests, vital objects of the state use the internet as a means to be interconnected, must think about protecting the vital objects of the state/state interests in the cyber world. Protection acts of terror against the interests of the state where all state affairs, in general, use the internet, need to be thought of as an anticipatory step and a countermeasure step.

ICILS 2020, July 01, Semarang, Indonesia
Copyright © 2021 EAI
DOI 10.4108/eai.1-7-2020.2303611

Cyberterrorism in various literature is a form of terror attacks through the cyber world. Some interpret that cyberterrorism is a form of internet abuse that causes widespread computer network damage without spreading actual fear. Various definitions of cyberterrorism make experts interpret that cyberterrorism is an act of terrorism also as ordinary cybercrime crimes. The meaning of cyberterrorism, which classifies that cyberterrorism is an ordinary cybercrime crime, influences how it is handled or anticipated. How to handle it seems slow and less dangerous. If seen, the cyber / internet world is very likely with the transformation of the terror network that the initial membership is limited to certain areas turned into mass and global scale..

From the description above, it is necessary to anticipate the handling of cyberterrorism through criminal policy by understanding the meaning of cyberterrorism comprehensively. The network is positively correlated to terror propaganda and massive computer network attacks that can paralyze life's connections.

2. Method

The method in this article is a normative juridical method [1], using literature study. The legal material used in this article is legislation both domestically and abroad. The approach in this article is a policy approach with a comparative approach.

3. Result and Discussion

3.1. Cyberterrorism Crime Countermeasures Policy through Penal Efforts

a. Positive Criminal Law Instrument

One effort to tackle crime is to establish an act as a criminal offense. Indonesian criminal law regulates cybercrime in Law Number 11 of 2008 concerning Electronic Information and Transactions (EIT law). The formulation of cybercrime can be found in criminal provisions stipulated in Chapter XI Article 45 to Article 52, where criminal provisions in the EIT Law are formulated separately between prohibited acts and sanctions. For prohibited acts regulated in Chapter VII Article 27 to Article 37. The act of cyberterrorism can be identified in Article 30 in conjunction with Article 46 of the ITE Law, namely accessing computer networks without rights (unauthorized access to computers and services). Then Article 31 jo Article 47 of the ITE Law, which regulates illegal hacking and tapping. Then Article 33 jo Article 49 of the ITE Law, where acts that are prohibited and threatened by criminal actions are acts that cause computers not to work properly (cybersabotage). These actions if carried out on vital infrastructure such as transportation, telecommunications, banking and other infrastructure that control the lives of many people can be categorized as cyberterrorism. Moreover, these actions cause widespread fear.

b. Comparative Study

Some countries regulate cyberterrorism in the provisions of the Criminal Law Act. Like Australia, Germany and Turkey[2].

Australia regulates cyberterrorism in the Australian Penal Code (Criminal Code Act 1995). The Criminal Code Act 1995 includes terrorist acts from The Security Legislation Amendment (Terrorism Act 2002) in Article 100.1 (1) and Article 100.1 (2). Terrorist acts in Article 100.1 (1) are: (1)

(a) .....

(b) the action is done or the threat is made with the intention of advancing a political, religious or ideological cause; and

(c) the action is done or the threat is made with the intention of:

(i) coercing, or influencing by intimidation, the government of the Commonwealth or a State,

Territory or foreign country, or part of a State, Territory or foreign country; or

(ii) intimidating the public or a section of the public. ‘

The Criminal Code Act (s. 100.1 (2)) further states that an action will fall within the definition of a 'terrorist act'

if it:

(a) causes serious harm that is physical harm to a person; or

(b) causes serious damage to property; or

(c) causes a person's death; or

(d) endangers a person's life, other than the life of the person taking the action; or

(e) creates a serious risk to the health or safety of the public or a section of the public; or

(f) seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to:

(i) an information system; or

(ii) a telecommunications system; or

(iii) a financial system; or

(iv) a system used for the delivery of essential government services; or

(v) a system used for, or by, an essential public utility; or

(vi) a system used for, or by, a transport system. '

Further explanation regarding cyberterrorism is emphasized in Article 100.1 (2), where a terrorist act is a cruel act of entering, disrupting or damaging an electronic system that is not limited to information systems, telecommunications systems, financial systems, government service systems, vital public systems, or transportation systems.

Cybercrime and abuse of computer networks in Germany are listed in several Articles in Strafgezetzbuchs. Some articles that can be identified as cyberterrorism offenses are Article 202 a: Data Espionage, 263 a: Computer fraud; 269 Fraud or falsification of legally relevant data; 270 Deception or cheating in legal relations through data processing; 303 a: Alteration of data, 303 b: Computer sabotage.

Cyberterrorism in Turkey is regulated in Articles 243 and 244 of the Turkish Penal Code. (2)Article 243 Turkish Penal Code regulates Access to data processing systems. Article 244 "Hindrance or destruction of the system, deletion or alteration of data" is cybercrime, but if carried out by terrorists or aimed at terror, then cyberterrorism can be categorized as a cybercrime. However, when these crimes are committed by terrorists or reaching the aims of terrorists, they can be called cyber terror offenses.

c. Draft Criminal Code (Ius Constituendum)

The Penal Code draft defines the expansion of the territorial principles in Article 4 (c) for criminal offenses in the field of technology and information or other criminal offenses, which are consequently experienced or occur in Indonesian territory or Indonesian ships or aircraft. Then the passive national principle Article 5 (b-7) protects the country's interests related to the safety or security of electronic communication equipment. Meanwhile, offenses that can be categorized as cyberterrorism are regulated in Chapter V Criminal Acts Against Public Order, among others: 1. Tapping speech in a closed room with assistive or technical tools (article 302); 2. Install technical aids for listening / recording the conversation (Article 303); 3. Recording (owning / broadcasting) pictures with technical aids in the room for the public (Article 304). Then Chapter VIII (Crimes that endanger the Public Interest for People, Goods, and the Environment): 1. access computers without rights (Article 378); 2. Article 381 (Accessing computers without rights by damaging).

Based on the description above, the regulation of cyberterrorism, based on studies in the ITE Law, comparative studies, Germany, Turkey, and the Criminal Code Draft, classifies cyberterrorism as part of cybercrime. However, Australia, classifying sui generis, cyberterrorism is part of a criminal act of terror that uses computer facilities and cyberspace. Thus, To overcome cyberterrorism, if it has done by terrorists, cyberterrorism should be categorized as a criminal act of terror that uses computer/cyberspace facilities.

2. Policy on Preventing Cyberterrorism Through Non-Penal Means (Non-Criminal Law)

a. Non-Penal Policy in The ITE Law

The ITE Law regulates non-penal policies in preventing cybercrime, which in this case, also includes cyberterrorism. It is regulated in chapter VIII of civil dispute resolution and Chapter IX regarding the government and the community's role. Dispute resolution is regulated in Articles 38 and 39 of the ITE Law, whereas Article 38 (1) of the ITE Law regulates claims for compensation against parties who operate the Electronic System and use Information Technology that causes losses. Then Article 38 (2) stipulates that each community may file a lawsuit in a representative manner against the party that organizes the Electronic System and/or uses Information Technology, which results in detrimental to the community, by the provisions of the Laws and Regulations. Article 39 (1) states that a civil claim is carried out by the applicable laws and regulations, then Article 39 (2) regulates the settlement of disputes through the arbitration body and other alternative dispute resolution solutions. In Chapter IX, Article 40 states that the government is obliged to facilitate, protect the use of technology and information, and determine agencies or institutions that have strategic electronic data that must be protected, and agencies or institutions that have strategic electronic data are required to make electronic documents and make backups and then connect them to a particular data center. Article 41 of the ITE Law regulates public participation in the use of information technology by forming consultative and mediating institutions.

It appears in the ITE Law Articles 40 and 41 using a technological approach in securing electronic data. Given the limitations of criminal legal means in preventing crime. Factors that can provide loopholes / opportunities for the occurrence of cyberterrorism are not enough to be done utilizing criminal law but the positive use of technology needs to be done.

b. Deradicalization and Utilization of Educated Staff Policies

Terrorism is inseparable from a wrong understanding of studying religious teachings or interpreting something wrong concerning particular political views. Therefore the need for de-radicalization of religious views that are not following what should be. It can be achieved by strengthening social ties (family, community, educational environment), giving a real understanding of the teachings of religion so that defending religious teachings does not need to hurt or kill other people who are not faithful. Then, cyberterrorism is caused by smart human factors but not utilized. Increasing the number of people who have no hope because of the process of social integration, also worsening social inequalities. (3) Then, cyberterrorism is caused by smart human factors but not utilized. Increasing the number of people who have no hope because of social integration also worsens social inequalities.

3. Conclusion

Based on the discussion above, the conclusions that can be drawn in this paper are:

1. Cyberterrorism prevention/control policies through means of punishment can be viewed from the attitude of some countries in regulating actions that can be categorized as cyberterrorism. Cyberterrorism criminal acts in positive criminal law have not been explicitly criminalized but can be identified in which actions fall into the category of cyberterrorism such as Law No. 11 of 2008. Likewise, with some comparative studies such as Germany and Turkey as well, also in the Criminal Code Concept. Generally, it still categorizes actions that can be identified by cyber terrorism as a type of ordinary cybercrime. Australia is slightly different in formulating cyberterrorism acts. Australia formulates cyberterrorism as an act of terrorism using computer facilities and cyberspace so that Australia considers cyberterrorism to be part of an act of terror. Considering the nature and danger of acts of terror, the Indonesian government should place cyberterrorism as part of a terrorism crime.

2. The policy of preventing cyberterrorism through non-penal means (non-criminal law) is carried out through civil lawsuits in Articles 38 and 39 of Law no. 11 of 2008, then Articles 40 and 41 concerning the role of government and society, where the government protects the use of technology and information by establishing agencies and institutions with strategic data and information. The community also participates in the use of technology and information by forming consultative and mediating institutions. Then the approach of deradicalization and utilization of educated personnel is a policy effort.

Acknowledgments

Acknowledgments The author wishes to thank the Dean of Faculty of Law Universitas Negeri Semarang for providing a facility to join International Conference in ICILS 2020 UNNES

References

[1.] **Soekanto, Soerjono**, *Pengantar Penelitian Hukum*, UI Press, Jakarta, 1981

[2.] **Prasad, Krishna.** *Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework.***.** s.l. : Proceedings of the 3rd Australian Counter Terrorism Conference, 2012.

[3.] **Yaila, Mehmet.** *Cyber Terrorism From The Criminal Law Perspective.* 1, s.l. : Law & Justice Review, 2014, Vol. V.

[4.] **Arief, Barda Nawawi.** *Bunga Rampai Kebijakan Hukum Pidana.* s.l. : Radjagrafindo, 2008.