Available online at: http://jurnal.uns.ac.id
Yustisia Jurnal Hukum
| ISSN (Print) 0852-0941 | ISSN (Online) 2549-0907 |

Cyberterrorism Challenges: The Need for Global Mutual Legal Assistance for Universal Criminal Jurisdiction

Yasniar Rachmawati Madjid
Faculty of Law, Brawijaya University
Corresponding author's email: yasniar@ub.ac.id

Article Information

Submitted : July 10, 2021
Reviewed : September 25, 2021
Revised : November 11, 2021
Accepted : December 10, 2021

Keywords:
criminal jurisdiction;
cyberterrorism;
mutual legal assistance

DoI: 10.20961/yustisia.v10i3.54953

Abstract

Terrorism is a crime that involves more than one state in an attack on world peace and security. The handling of international terrorism is not only based on national law but also on international law. With widespread concerns about cyberterrorism and the frequent use of the term "cyberterrorism" at present, many international organizations have made efforts to combat this threat. Since cyberterrorism is an international crime, local regulations alone are not able to defend against such attacks; this requires mutual legal assistance among states and a transnational response. Therefore, an attacked country will invoke international law to seek justice for any resulting damage through the exercise of universal jurisdiction. Cyberterrorism cannot be prevented only with national regulations; international cooperation among states is necessary to prevent and defend against cyberterrorism attacks. This article discusses about cyberterrorism as a transnational/international crime. It should be subjected to universal jurisdiction through multinational cooperation, and this would be the most suitable method to counter future transnational crimes, including cyberterrorism.

I. Background

The presently rapid development of technology and information provide facilities for people in committing actions in order to meet their needs. This usage of technology and information is utilized by people in enabling access to communication with other people, both within the boundaries of a state and across the boundaries of states. However, this development of technology and information is also utilized to enable access to crime within state boundaries and across state boundaries. One of the crimes that in its development is conducted by utilizing developments in technology is the crime of terrorism, which is more commonly recognized by the term of "cyberterrorism".

Terrorism utilizes planned threats or violence that is committed by individuals or sub-national groups with political or social objectives through intimidation toward a greater portion of society other than the direct victims (Sukarwarsini Djelantik, 2010). There are two primary characteristics in the definition of modern terrorism, which are threats or violence as well as socio-economic objectives. Without threats or violence being present, terrorists cannot compel decision-makers, in this case the government, to respond to their demands. In addition, without socio-political motivation, acts of violence are simply ordinary crimes and not terrorism. The crime of terrorism does not stand alone, because there are always matters that are related to the crime of terrorism itself. The matters that are related to terrorism include the illegal entry of residents across states (migration) and the trade of narcotics and drugs as well as conventional and strategic nuclear, chemical, and biological weapons that are known as weapons of massive destruction. These matters lead to the recognition of terrorism as an international issue that has implications of broad threats to human security (Richard O. Spertzel, 2002).

Based on the background of these objectives, it becomes unsurprising that international terrorist organizations possess the characteristics of being considerably organized, resilient, extreme, exclusive, and closed-in, as well as having very high commitments and special armies, and being supported by massive amounts of finances and funds.

Terrorism constitutes one of 22 international crimes (M.Cherif Bassiouni, 1986) and is included as one of the crimes that fulfill the criteria as a "*hostis humanis generis*" (general human enemy). In the discussion of the draft of the 1998 Rome Statute on the International Criminal Court, terrorism and drug trafficking were included as crimes that were suggested to be put under the jurisdiction of the ICC. However, this was rejected by most of the parties to the Rome Convention with the consideration that both of these crimes have been regulated in their own conventions, and thus the implementation of law enforcement toward these two crimes is left up to the national jurisdiction of each of the states that are involved.

Terrorism at present not only constitutes a local or national crime, but also has constituted a transnational and even international crime. Terrorism has become a crime that is international in nature, quite threatening or dangerous toward security and peace, and very much detrimental to the welfare of societies and nations. The events of the September 11 attacks and the first and second Bali bombings have led the global society to regard terrorism as an international enemy. The mass killings have united the world against international terrorism.

Since the phenomenon of terrorism became a discussion on the international scale, experts have taken the view that developments in the globalization era also have affected the developments of terrorist movements. Globalization influences the development of communication technologies that in the end leads to the creation of a world of communication based on computers, which in everyday life is recognized as the Internet.

The existence of the Internet is formed through computer networks that connect countries or continents over the Transmission Control Protocol/Internet Protocol (TCP/IP). The Internet is illustrated as a collection of computer networks that is composed of a number of smaller networks that all possess different network systems (Maskun, 2013). With the Internet as "the network of networks" that reaches all parts of the world, this allows for the creation of a new space or world that is called "cyberspace". Cyberspace is believed as a global structure or communicative space in which no country has the right to regulate the content of information that is desired to be communicated between two people or among many people (Edmon Makarim, 2003).

Furthermore, the Internet (cyberspace) itself may be regarded as the two sides of a coin. On one hand, the Internet with its various benefits aids the development of a state and allows for the easy distribution of information that enables to keep the global society up to date, but on the other hand, the Internet also provides opportunity to people who possess the motivation or desire to commit acts of crime.

The networks of the Internet are utilized by actors of terrorism to support their terrorist activities; this usage of the Internet by terrorists is recognized by the phrase "terrorists use the Internet". This usage is quite similar to that of other users of the Internet. They utilize the Internet to communicate with each other and to seek supporters by spreading propaganda through web sites on the Internet. They also utilize the Internet to spread or distribute information (photo, audio, video, and software) of, and seek information for, their activities of terrorism. George Tenet, the Director of the Central Intelligence Agency (CIA), has stated that terrorist groups, including the groups of Hezbollah, Hamas, and Al-Qaeda, have utilized computerized files, e-mail, and encryption to support their operations. Terrorists have also utilized the Internet to conduct business transactions to finance their activities as well as to commit other cybercrime acts.

Further, the usage of the Internet by terrorists or groups of people to commit crimes of terrorism is known as cyberterrorism. In several pieces of literature on international law, it has been mentioned that cyberterrorism has become a part or a form of cybercrime. Through the usage of the Internet, terrorists can easily conduct cyber-attacks, as through the Internet, they are unable to be identified. Terrorists possess many advantages when conducting cyber-attacks through the Internet. In contrast to acts of terror that utilize bombs, where the terrorists must be present at the place of the attack, with the Internet, terrorists can execute their acts without having to be at the place of the attack.

This new form of the crime of terrorism in the form of cyberterrorism has had influences on the legal regulations that apply in different countries as well as international law, because regulations regarding terrorism, whether those of national, regional, or international law, do not clearly regulate the usage of technology in the execution of acts of terror.

Next, from the elements of their actions, acts of cyberterrorism that are presently occurring may be divided into two types, which are national cyberterrorism and

international cyberterrorism. National cyberterrorism comprise acts of terrorism that are conducted within the scope of a single state, which are conducted utilizing networks of computers and digital information and possess targets (of state), actors, and victims originating entirely from the state where the crime occurred. Meanwhile, international cyberterrorism is terrorism that involves nationals or regions of more than two states. Involvement in this case may be understood as pertaining to actors of crimes of terrorism or victims of crimes of terrorism that are committed with information systems.

On the other hand, regarding regulations on cyberterrorism, there have not been specific regulations in international law, and thus presently there exists a legal void regarding the regulation of the crime. Meanwhile, there are several regional and international regulations that are applied in the cases of cyberterrorism that have happened, including the ASEAN Convention on Counter-Terrorism and the International Convention for the Suppression of Terrorist Bombings.

Acts of cyberterrorism that are presently occurring fulfill elements of international crime (M.Cherif Bassiouni, 1986):

1. The actions that are forbidden have significant consequences for international interests. Examples of international crimes that fulfill this element are genocide and crimes against humanity.
2. The actions that are forbidden comprise depraved actions and are considered threatening to values that are collectively followed by the global society, including what has been considered historically as actions that touch the human spirit.
3. The actions that are forbidden possess transnational inspiration that involves or affects more than one country in the planning, preparation, or execution, whether according to the diversity of nationality of the actors or victims of the crime, or the utilized equipment that transgress state boundaries.
4. The actions jeopardize protection toward international interests or toward people who are protected internationally.
5. The actions violate international interests that are protected but not to the extent as stated in the first and second points, but because of their basic nature, the actions may be prevented and suppressed through international criminalization.

Considering the elements of international crime above, cyberterrorism meets three of the five elements. Cyberterrorism is an international crime of terrorism that comprises actions that attack international interests, which are reflected by actions that attack civilians not as the objective but simply as a way for achieving the interests of the terrorist group, as well as involvement of more than two countries in relation to actors, victims, regions, weaponries, and international funding for the activity. According to the second view of Bassiouni, cyberterrorism also fulfills international elements that must be fulfilled for an international crime, in that terrorism is a crime that involves more than one state and attacks world peace and security both directly and indirectly, and thus the handling of cyberterrorism is not only based on national law but also international

law. In light of the characteristics of the crime of international terrorism above, states have organized international cooperation to handle the crime. Yet, the effectiveness of cooperation to freeze terrorist assets and to prevent money laundering very much depends on the global commitment. The ineffectiveness of international cooperation is caused by the emergence of dilemmas of democratic states, in particular for the issue of human rights. Policymakers at the national level need to place mutual security above the sovereignty of the state.

There are at least three factors that cause governments to have difficulties in creating international cooperation (Sukarwarsini Djelantik, 2010):

1. The forces that governments possess give a false sense of security to the people. The number of personnel, military equipment, and the strength of national defense convince the people that international coordination and cooperation are not necessary.
2. There are no agreements among governments regarding which groups are terrorist groups and which ones are not.
3. Governments and terrorists possess different timeframes. In a democratic state, the political interests of government officials are outlined through the next general election and the possibility of becoming re-elected. Because governments change, agreements with terrorists that have been made by the previous government have the possibility of becoming deprecated. In contrast, terrorist leaders are not time-limited and thus assume that cooperation agreements within the group will still continue. Consequently, terrorists design long-term agendas and possess a greater political advantage compared to the government.

Another effort of international cooperation in facing cyberterrorism is through extradition. Cyberterrorism does not recognize state boundaries, while governments do recognize boundaries and can only work within the limits of jurisdiction of certain states. Otherwise, there is no agreement in the definition regarding these acts of terrorism, and this is what makes extradition difficult to be conducted.

Other efforts for handling the cases are conducted through the organization of the UN to create international agreements to detain and extradite terrorists from the states that protect them. Yet, there is a difference in viewpoints regarding the characteristics of freedom fighters compared to terrorists. The method of resolution is with the creation of bilateral agreements among the states that possess interests. However, these bilateral agreements do not provide much effectiveness in the handling of the cases, considering the spread of crimes of international terrorism that is unpredictable. Therefore, it becomes necessary to implement regulation through multilateral international agreements that possess integral responsibility as a form of accountability of states in the world, as regulated in the Rome Statute of the International Criminal Court that regulates the enactment of Universal Jurisdiction in the handling of criminal cases that possess elements of international crime, such as the elements that are present in crimes

of cyberterrorism. This application of universal jurisdiction needs to be conducted to provide clear guidance for states in the handling of crimes of cyberterrorism that have international impacts and criminal elements, as well as to suppress these crimes. Additionally, it becomes necessary to regulate the harmonization of legal regulations and authority between national law and international law regarding the application of universal jurisdiction in the handling of crimes of cyberterrorism.

This article is to respond to the issue regarding the regulation of cyberterrorism in international law and the urgency for the application of universal jurisdiction in the handling of crimes of cyberterrorism in international law. The objective to be achieved in this article is to find out and analyze the existing legal void in regulations regarding cyberterrorism in international law and thus to be able to analyze the urgency of the application of universal jurisdiction toward crimes of cyberterrorism.

II. Method

This article comprises a normative legal research that utilized the legal conceptual approach and the statute approach. The primary legal materials that were utilized are international regulations related to cyberterrorism and the application of universal jurisdiction. This article also utilized the legal material analysis technique of prescriptive analysis and the method of legal syllogism and conceptual approach to draw conclusions.

III. Discussion

1. Regulation of International Cyberterrorism in International Law

Terrorism is not a new issue in international relations that concern states, as well as an intriguing issue for the international community, whether terrorism at a domestic level or at the international scale. The former has relations to power struggles in a country among different groups of interests, while the latter reflects the existence of conflicts of interest from foreign parties or other countries toward a state (Poltak Partogi, 2003).

The international stipulations that define terrorism are the Convention for the Prevention and Punishment of Terrorism as adopted by the League of Nations. Article 1 (2) of the Convention states (Illias Bantekas, 2003):

…acts of terrorism [as] criminal acts directed against a State and intended or calculated to create a state of terror in the minds of particular persons, or groups of persons or the general public.

Many views have attempted to define terrorism, one of which being the understanding contained in Article 14 Paragraph 1 of the Prevention of Terrorism (Temporary Provisions) Act, 1984, as the following (Loebby Loqman, 1990):

"Terrorism means the use of violence for political ends and includes any use of violence for the purpose of putting the public or any section of the public in fear."

Activities of terrorism have the objective to make other people feel afraid, and in that way are able to attract the attention of people, groups, or countries. Usually, acts of terror are utilized if there are no other paths that may be taken to carry out their objectives. Terrorism is utilized as a psychological weapon to create an environment of panic and uncertainty, to create disbelief among the people toward the abilities of the government, and to force certain people or groups to obey the intents of terror actors.

The word "terror" entered political vocabulary during the French Revolution. At the end of the 19th century just before World War II, terrorism became a technique for revolution, such as in the Stalin regime in the 1930s, which is called a regime of terror. In the Cold War era, terror was linked to the threat of nuclear weapons.

Terrorism possesses the following characteristics:

1. It comprises forced intimidation.
2. It utilizes murder and destruction in a systematic manner as a facility for certain objectives.
3. Victims are not the objective, but a facility to create a war of nerves, which is to kill one person to scare a thousand.
4. Targets of acts of terror are chosen while working in secret, but the objective is publicity.
5. The message of the acts are quite clear, even though actors do not always declare themselves personally.
6. The actors are mostly motivated by idealism that is quite strict.

At present, crimes have developed through other media for carrying out objectives. One of the facilities that are utilized by perpetrators is the usage of electronic media, which leads to crime called "cybercrime". Cybercrime comprises forms of crimes that arise because of the utilization of Internet technologies. Several views consider cybercrime and computer crime to be identical.

The U.S. Department of Justice provides the understanding of "computer crime" as "an illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution."

This understanding is identical to that given by the Organization of Europe Community Development, who defined computer crime as "any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data (Dikdik M. Arief Mansur and Elisatris Gultom, 2009)."

The Report of the 10th UN Congress in Vienna, on 19 July 2000, utilized the term "computer-related crime", which comprises the following two forms of understanding: "The term 'computer-related crime' had been developed to encompass both the entirely new forms of crime that were directed at computers, networks, and their users, and the more traditional form of crime that were now being committed with the use or assistance of computer equipment".

Cybercrime is a form of crime that is relatively new in comparison to other forms of crimes that are conventional in nature (street crime). Cybercrime emerges in line with the development of technology, in particular in the field of telematics. Considering the form of the crime, cybercrime itself contains several specific characteristics:

1. Non-violence.
2. Minimization of physical contact.
3. Usage of technology.
4. Utilization of networks of global telematics (telecommunication, media, and informatics).

The usage of technology and networks of global telematics allows for cybercrime to be conducted by anyone and anywhere, affecting any place. Cybercrime is crime that does not recognize territorial or state boundaries.

According to M. Cherif Bassiouni (Erwin Aswandi, 2013), there are fundamental differences between transnational crime and international crime. Transnational crime refers more to crime for which its nature transgresses the territorial boundaries of states (borderless) and has impacts on more than one country. From this, it can be understood that cybercrime may be categorized as transnational crime, which is then regulated in the United Nations Convention against Transnational Organized Crime (Palermo Convention) of November 2000 and ASEAN Declaration of 20 December 1997 in Manila.

The usage of electronic media in a crime is also involved in the crime of terrorism that is called cyberterrorism. The term "cyberterrorism" had been introduced since 1997 by Barry Collin (Dorothy E. Denning, 2009), a senior researcher at the Institute for Security and Intelligence in California in the United States. In the view of Collin, computerization in various fields of human life creates a new vulnerability. This vulnerability may be exploited for acts of terrorism, whether through destruction, alteration, and acquisition and retransmission, for which the objective is to cause chaos and terror.

In the previous discussion, it has been explained that cyberterrorism is one of the forms of cybercrime. From a conceptual standpoint, cyberterrorism is not much different from "traditional" terrorism, except that it contains the element of "cyber". Several researchers have taken the view that activities of terrorism in

cyberspace are considered as cyberterrorism (Zahri Yunus and Rabiah Ahmad, 2012).

As with the definition of terrorism, there is not yet a standard definition for cyberterrorism. There are several views among researchers regarding the definition of cyberterrorism. Denning defines cyberterrorism as "unlawful attacks and threats of attack against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives (Gabriel Weimann, 2014)."

From this understanding, it may be construed that cyberterrorism is "actions against the law and threats of attacks toward computers, networks, and information stored within them, if conducted to intimidate or compel governments or people in supporting a political or social objective." Denning also explained that to be categorized as cyberterrorism, the act of attacking must cause violence toward people or property, or at the least cause fear to emerge (D. E. Denning, 2000).

The CRS Report for Congress defines cyberterrorism as "the use of computers as weapons, or as targets, by politically motivated international, sub-national groups, or clandestine agents who threaten or cause violence and fear in order to influence an audience, or cause a government to change its policies" (C. Wilson, 2015). This means that cyberterrorism is stated as the usage of threats without legally recognized authority, as well as violence or disruptions toward cyber systems. The results may be in the form of death or injury to a person or several people, physical damage, civil unrest, or economic losses to a substantial degree.

Among others, there are several interpretations regarding cyberterrorism from various sources:

1. Cyberterrorism is a kind of criminal action that is conducted through computers and results in crime, death, and/or destruction, and causes terror for the intent of forcing the government to change policies (Lukasz Jachowicz, 2013).
2. Cyberterrorism is the usage of computer networks as a tool to shut down important national infrastructure (such as energy, transportation, and government activities) or to coerce or intimidate the government or civil population (James A. Lewis, 2002).
3. Cyberterrorism, as with other acts of terrorism, comprises an act of crime that is conducted with careful planning with little effort that is usually difficult to be identified or caught, which is utilized to interfere in the functioning of civil society (Bill Clark, 2011).

From the interpretations above, it can be concluded that cyberterrorism is a criminal act that is conducted by a person, a group of people, or an organization that utilizes computer network systems or targets those computer network

systems, which causes damage or intimidates the government or the public for political, social, or economic objectives, or damage to the infrastructure of a state. Cyberterrorism itself is still presently categorized as a transnational crime; however, there are not yet any specific international regulations that deal with the crime of cyberterrorism. For the handling of this crime, international regulations and state practices exist to be applied, although they do not specifically regulate regarding cyberterrorism.

1.1. International Agreements

1.1.1.2000 Palermo Convention

This convention contains regulations on transnational crimes that possess the following elements, as explained in Article 1 of the convention:

a. Conducted in more than one country;
b. Conducted in one country, but the important parts of activities of preparation, planning, direction, or control occur in another country;
c. Conducted in one country, but involves a group of organized crime that is involved in criminal activities in more than one country; or
d. Conducted in one country, but has primary effects in another country.

As a case example, in 1998, a guerrilla terrorist group sent e-mails amounting to 800 e-mails per day to the government of Sri Lanka, containing the text "we are the Internet Black Tiger and we are doing this to disrupt your communications." This indicates that the guerilla group has the capability of sending e-mails from another country, but the impact is on the country of Sri Lanka. In line with Article 1 above, cyberterrorism may be conducted in one country but has primary effects in another country, and thus in light of this fact, cyberterrorism is included in transnational crimes under the sub-heading of cyberterrorism, which in the above case would be cyberterrorism against government.

In the handling of transnational crimes, an indirect enforcement system may be implemented, which involves indirect handling through international cooperation. The bulk of the enforcement efforts in international cooperation for the handling of transnational crimes such as cyberterrorism is regulated in Article 27 of the Palermo Convention, which states that countries are required to work in line with their respective legal systems and national governments, in order to improve the effectiveness of handling the crimes that are covered by the Convention.

1.1.2.Convention on Cybercrime/Budapest Convention

This convention regulates criminal sanctions for perpetrators of cybercrime, which is left up to each state, considering that cyberterrorism is a transnational crime that is inescapable from the national law of each state. This is in line with Article 13 of the Convention on Cybercrime:

"(1) Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

(2) Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measure a, including monetary sanctions."

This article delegates that in its regulation, criminal sanctions may be given by the state toward individual perpetrators of cybercrime in the form of revocation of freedom (punishment, imprisonment) and even financial sanctions. Although this convention does not explicitly regulate cyberterrorism, perpetrators of the crime of cyberterrorism may be charged accordingly by these situations:

a. Illegal Interception, which is the listening or recording of auditory transmission that is not directed to the public covertly into computer systems with technical assistive instruments.
b. Data Interface, which includes data theft or destruction, which are often liable for perpetrators of cyberterrorism in addition to spreading terror.
c. Computer Related Offences, including data forgery and disruption of intended computer functions.

The following articles explain in more specific details regarding charges that may be levied on perpetrators of cyberterrorism. Article 2 regulates illegal access, which is the retrieval of data in an unauthorized manner with malicious intent that is against the law, or in relation to computer systems and in connection with other computers. Next, Article 3 regulates illegal interception in an unauthorized manner, through certain techniques, with transmissions of computer data that are not public property, and from or within a computer system, including electromagnetic emissions from a computer system that contains the data of the computer.

1.1.3.2017 ASEAN Declaration to Prevent and Combat Cybercrime

This is a cooperative ASEAN declaration to handle and prevent the occurrence of the criminal acts of cybercrime. Cybercrime itself is composed of Unauthorized Access to Computers and Services, Illegal Contents, Data Forgery, Cyberterrorism, Cyberespionage, Extortion, Hacking, and Cyber-Porn (Ferddy Haris, 2009).

1.1.4. International Convention for the Suppression of Terrorist Bombings

This convention was adopted by the UN General Assembly on the date of 15 December 1997 in A/RES/52/164. This convention limits that terrorists themselves have the objective to bomb a structure and not just to spread radical ideologies. The relation of this convention to cyberterrorism is found in Article 2, which states that:

"Any person commits an offence within the meaning of this Convention if that person unlawfully and intentionally delivers, places, discharges or detonates an explosive or other lethal device in, into or against a place of public use, a State or government facility, a public transportation system or an infrastructure facility:

a. *With the intent to cause death or serious bodily injury; or*
b. *With the intent to cause extensive destruction of such a place, facility or system, where such destruction results in or*
c. *is likely to result in major economic loss."*

As explained in the previous discussion, cyberterrorism brings together the element of terrorism in the traditional sense in combination with the element of "cyber" or technology, and thus by regulations regarding terrorists, they may be charged by regulations related to traditional terrorists, with several required interpretations. By Article 2 above, it is stated that every person who commits a crime against the law according to this convention has the intention of setting or activating a bomb or other killing device toward public facilities, state or government facilities, public transportation, or infrastructure. Then, in Article 1(3), it is explained that:

"explosive or other lethal device: An explosive or incendiary weapon or device that is designed, or has the capability, to cause death, serious bodily injury or substantial material damage;..."

This article explains that the explosions involve the usage of a tool that is utilized to commit crimes of terrorism. Regarding cyberterrorism, the crime may be charged with the two articles, as Article 2 has clearly explained about the people or legal subjects, while Article 1(3) explains

regarding tools, which in the case of cyberterrorism, the utilized tools comprise mobile phones, computers, and other similar technologies. Thus, when interpreted extensively, Article 2 *juncto* 1(3) may be utilized to charge perpetrators of cyberterrorism.

1.1.5. 2007 ASEAN Convention on Counter-Terrorism

This convention was created on 13 January 2007 by the member states of ASEAN. The objective of forming this convention is to eradicate all forms of the crime of terrorism. As such, Article 1 declares that:

"This Convention Shall provide for the framework for regional cooperation to counter, prevent and suppress terrorism in all its forms and manifestations and to deepen cooperation among law enforcement agencies and relevant authorities of the Parties in countering terrorism."

In Article 1, it is explained that the convention becomes the legal framework for the cooperation to eradicate and restrain terrorists and all the forms that they may take. These forms of manifestations may be construed as cyberterrorism, which over the course of time and the development of advanced technologies leads to a new relational manner of terrorism.

This convention also regulates cooperation (the Indirect Enforcement System) in the enforcement for the eradication of terrorism and all the manifestations in Chapter VI. Then, Chapter VII explains sanctions for perpetrators of crimes of terrorism and all the manifestations, with usage of the respective jurisdiction and the national law of the state. Chapter XIII regulates the extradition of perpetrators of crimes of terrorism and its manifestations.

1.1.6. 1999 International Convention for the Suppression of the Financing of Terrorist Bombings

This convention was adopted by the General Assembly of the United Nations in Resolution 54/109 on the date of 9 December 1999. In this convention, what is regulated is the funding of terrorism that is not part of the act of terrorism, and thus what is related to the funding of cyberterrorism. Article 2 may be linked to cyberterrorism in relation to funding:

"Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

(a) *An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or*

(b) *Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act."*

The article means that every person commits violations in relation to this convention in any way, whether directly or not, against the law and intentionally, in providing or collecting funds if the funds are intended or known to be utilized for terrorism. Regarding the collection of funds, cyberterrorism that utilizes technology may be charged by this article because of the phrase "by any means" (in any way).

1.1.7.2005 International Convention for the Suppression of Acts of Nuclear Terrorism

The Convention on Nuclear Terrorism is a treaty by the United Nations that was created in 2005 and is designed to criminalize acts of nuclear terrorism as well as to promote police and judicial cooperation to prevent, investigate, and punish these actions. This treaty contains an article related to cyberterrorism, which would be Article 2 (1):

"*Any person commits an offence within the meaning of this Convention if that person unlawfully and intentionally:*

(a) Possesses radioactive materials or makes or possesses a device:

(i) With the intent to cause death or serious bodily injury; or

(ii) With the intent to cause substantial damage to property or to the environment;

(b) Uses in any way radioactive materials or a device, or uses or damages a nuclear facility in a manner which releases or risks the release of radioactive material:

(i) With the intent to cause death or serious bodily injury; or

(ii) With the intent to cause substantial damage to property or to the environment; or

(iii) With the intent to compel a natural or legal person, an international organization or a State to do or refrain from doing an act."

In this article, a person who has radioactive materials, or creates or has a device (of such nature), may be charged with the article. The device here, as referenced in Article 1(4), refers to nuclear explosives, radioactive material distributors, or radiation emitters. This article may

be utilized to charge perpetrators of cyberterrorism when they assemble devices that are utilized to detonate nuclear materials or spread radiation that is intended to result in death or serious injury, or great damage to property or the environment.

1.1.8.Tallinn Manual 2.0

Cyber operations have continued to increase from 1990 to the present, and there have been technological developments in cyber operations. This has attracted much of the attention of different states because the actions are considered to have been detrimental to the states. As such, the NATO Cooperative Cyber Defense Centre of Excellence conceived regulations that are called Tallinn Manual 1.0 on the International Law Applicable to Cyberwarfare of 2013. Tallinn Manual 1.0 emphasizes on cyber operations that target the control of systems from enemies and focus on International Humanitarian Law (Zahra, I., & Wulan Christianti, 2021). Thus, Tallinn Manual 1.0 is designated for wartime conditions but not designated for cyber-securities such as cyberespionage, intellectual property theft, and other criminal activities that become serious disruptions for a state. Tallinn Manual 1.0 was composed based on international treaties, customary laws, and other legal bases, and has resulted in 95 black-letter laws that become guidelines for states in the condition of an occurring cyberwarfare, including the stipulations of within a neutral territory.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations is a continuation of Tallinn Manual 1.0, which is the result of discussions with an expert group that was initiated by the NATO Cooperative Cyber Defense Centre of Excellence, and was issued in 2017. Tallinn Manual 2.0 discusses regarding cyber activities related to cyberwarfare during times of peace with emphasis on cyber events that are faced by states, but under the level of cyber operations.

The Tallinn Manual contains the stages of a cyber-attack, which comprise (Pipyros, Kosmas, Lilian Mitrou, Dimitris Gritzalis, 2017):

a. Severity, which is the level of cyber-attack that is determined based on the scope, timeframe, and intensity of cyber operations;
b. Immediacy, determining the level of time proximity, which refers to the nearness of the consequences that emerge due to a cyber-attack;
c. Directness, which refers to immediate causes of cyber operations that lead to certain impacts;
d. Invasiveness, which refers to the degree to which cyber operations will disrupt the states to be attacked or the cyber systems of that state to a detriment;

e. Measurability of effects, which refers to the fact that as impacts become more measurable, it becomes easier for a state to assess the situation of whether cyber operations have been able to be considered to be at or to have achieved the level of "use of force" or not;

f. Military character, which is the cause-effect relationship between cyber operations and military operations that are very likely to be cyber-attacks that qualify as the "use of force";

g. State involvement, which is the level that refers to the relationship between a state and cyber operations. As the relationship between cyber operations and a state becomes clearer and closer, it becomes very likely that the situation will be considered as the "use of force";

h. Presumptive legality, which refers to the reality that international law, in general, comprises regulations that determine prohibitions of certain actions. Actions that are not forbidden will be permitted to be conducted. Thus, if there are no treaties that do not firmly contain prohibitions, or if there are no prohibitions according to international customary law, then an action in general should be considered to be a legal action.

In relation to cyberterrorism, the crime may also be charged with the regulations of both Tallinn Manual 1.0 and Tallinn Manual 2.0, because cyberterrorism may be conducted in conditions of war or conflict among states as well as in peaceful conditions as is presently occurring. Certainly, the conditions in the Tallinn Manual may be regarded as guidelines for states in handling crimes that utilize cyber operations, including cyberterrorism.

1.2. State Practices

In addition to international legal instruments for their handling, transnational crimes are not removed from the national law of each state. The following are several regulations regarding cyberterrorism in various states:

1.2.1.Cambodia

Cambodia has its own laws for regulating the handling of cybercrime. In its body of regulations, there exists several regulations that may be utilized to charge perpetrators of cyberterrorism, as with Articles 21-26 below:

a. Article 21: regulates Illegal Access, as access to computers in an illegal or unauthorized manner, such as obviating security or

hacking passwords; violators are punishable up to 12 years of imprisonment.

b. Article 23: regulates Illegal Interception, as unauthorized interception conducted in a technical manner, by the transmission of non-public computer data to, from, or within computer systems, including electromagnetic emissions from computer systems that contain the computer data; violators are punishable up to 7 years of imprisonment.
c. Article 25: regulates Unauthorized Data Transfer, as the illegal transfer of data from computer systems or through storage media for computer data; violators are punishable up to 12 years of imprisonment.
d. Article 26: regulates System Interference, as unauthorized actions that cause serious disruptions to the functions of computer systems, by inputting, transmitting, changing, deleting, or damaging computer data, or limiting access to that data; violators are punishable from 3 to 15 years of imprisonment and fined from 6 million Riel to 30 million Riel.

1.2.2.Belgium

In order to charge perpetrators of the crime of cyberterrorism, Belgium possesses a regulation in its penal code regarding cybercrime that is related to cyberterrorism, as the crime of hacking (Natsir, Nanda Ivan, 2009):

Article 550 (b) of the Criminal Code:

Section 1. Any person who, aware that he is not authorized, accesses or maintains his access to computer system, may be sentenced to a term of imprisonment of 3 months to 1 year and to a fine of (BFr 5,200-5m) or to one of these sentences. If the offences specified in Section 1 above is committed with intention of defraud, the term of imprisonment may be from 6 months to 2 years.

Section 2. Any person who, with the intention to defraud or with the intention to cause harm, exceeds his power of access to a computer system, may be sentenced to term of imprisonment of 6 months to 2 years and to a fine of (BFr 5,200-20m) or to one of these sentences.

Section 3. Any person finding himself in one of the situations specified in Sections 1 and 2 who either: accesses data which is stored, processed or transmitted by a computer system, or procures such data in any way whatsoever, or makes any use whatsoever … or causes any damage, even unintentionally, to a computer system or to data which is stored, processed or transmitted by such a system,

may be sentenced to a term of imprisonment of 1 to 3 years and to a fine of (BFr 5, 200-10m) or to one of these sentences."

This article allows for perpetrators of cyberterrorism to be charged in the case of those who access information systems without rights or illegally, if they conduct fraud with the information systems or if they cause damage to the data in the computers or information systems.

1.2.3.Singapore

Singapore possesses a special law outside of the penal code that regulates regarding cyberterrorism. The following are some of the legal stipulations of Singapore regarding cyberterrorism:

Unauthorized access to computer material.

Section 3-(1) … any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction … to imprisonment for a term not exceeding 2 years or to both and … in the case of a second or subsequent … for a term not exceeding 3 years or to both.

1. *If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.*
2. *Any person who causes a computer to perform any function for the purpose of securing access to … any computer with intent to commit this section applies shall be guilty of an offence.*
3. *This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years."*

Singaporean law states that every person who accesses computers without rights or in other words illegally, which may lead to crimes of cyberterrorism, is to be sentenced to prison.

Regulations regarding a crime that occurs in society, such as cyberterrorism, are very important and fundamental in the prevention and eradication efforts for the crime. The regulation of the crime in various legal regulations, specifically national law, comprises the implementation of state jurisdiction in order to provide protection for the people. Therefore, there needs to be specific regulations that regulate in detail regarding the definition, criminal elements, criminal scope, and legal authority for the crime of cyberterrorism. This becomes required, considering the ever-increasing number of acts of terrorism

through cyberspace and the obstacles that are faced by states in handling them because of the inexistence of certain guidelines for the handling of the crime. It is certain that these international regulations may be harmonized with the national laws of each state.

2. Application of Universal Jurisdiction toward the Crime of International Cyberterrorism

In addition to the urgency for the regulation of the crime of cyberterrorism into specific international regulations, there is another urgency for the handling of this crime. That urgency is for the ability to apply universal jurisdiction for the handling of the crime of cyberterrorism, which is to be realized with various treaties involving, and cooperation among, states that are affected by the impacts of the crime.

This application of universal jurisdiction is because of the sameness of characteristics of the crime of cyberterrorism with crimes against humanity, which are placed under the jurisdiction of the International Criminal Court, which also utilizes universal jurisdiction.

Cyberterrorism possesses the following characteristics:

1. Forced intimidation
2. Usage of systematic murder and destruction to facilitate certain objectives
3. Victims not being the objective, but the facility for a war of nerves by killing one person to scare a thousand
4. Terror act targets selected while working in secret, but with publicity as the objective
5. Clear messages of the acts, even without actors not always declaring themselves personally
6. Motivation of actors by strict idealism
7. Usage of information and computer or communication technologies to carry out the act

Cyberterrorism possesses specific characteristics that are not present in conventional crime, which is that it is carried out systematically and broadly, and is organized in an orderly manner. Cyberterrorism itself in its execution utilizes weapons of mass destruction; its usage of information technology leads to cyberterrorism being considered as a transnational issue that has the implication of a broad threat to human security. Considering the above characteristics, terrorism should be able to be categorized as "international armed conflict" because in reality, cyberterrorism attacks international interests in an organized manner and utilizes weapons. Cyberterrorism not only causes losses in the form of victims, but also can paralyze information systems that are

important for the state, such as networks of the government, hospitals, and state communications.

It is certain that the application of universal jurisdiction cannot be extended to all crimes of cyberterrorism, yet only to the crime of cyberterrorism on the international scale, or what is commonly called international cyberterrorism. The definition of international cyberterrorism has not been specifically regulated in an international regulation but may be summarized from the definition of "international terrorism", which:

"…is the systematic use, or threatened use of violence to intimidate a population or government and thereby effect political, religious or ideological change involving citizens or the territory of more than one country".

From the above definition, it can be understood that international terrorism is terrorism that involves the people or regions of more than two states. "Involvement" in this case may be understood to include perpetrators of the crime of terrorism as well as victims of the crime of terrorism. Certainly, the stipulation may be applied toward the crime of international cyberterrorism with the remark that the action is conducted with the usage of information technology, which has broader effects compared to conventional international terrorism.

The characteristics of this crime is the same as crimes against humanity, which are placed under the legal authority of the International Criminal Court, for which the following are the characteristics (Human Rights Watch, 2007):

1. The nature and character of the actions must be inhumane, causing very intense suffering, or serious bodily injury, or damage to physical and mental health.
2. The actions must be conducted as part of an attack that is systematic or widespread.
3. The act or attack is directed to civilians.
4. The attack must be conducted according to discriminative reasons with regard to nationality, politics, ethnicity, race, or religion.

The primary characteristic that is possessed by international cyberterrorism is that the crime of terrorism must involve people as both perpetrators and victims, as well as territories, of more than two states. Considering the similarity of characteristics of the crime of international terrorism and crimes against humanity, the crime of international terrorism may be classified as an international crime, and universal jurisdiction may be applied.

Jurisdiction itself is the authority that a state possesses to create legal regulations (prescriptive jurisdiction) and the authority to enforce a decision that is created based on the laws that had been created (enforcement jurisdiction).

State jurisdiction in the perspective of international law, according to Anthony Csabafi as quoted by Parthiana, may be defined as the following (I Wayan Parthiana, 2007):

State jurisdiction in public international law means the right of state to regulate or affect by legislative, executive, or judicial measure the rights of persons, property, acts or events with respect to matters not exclusively of domestic concern.

The emphasis of this jurisdiction is the place of the object. The object of jurisdiction may be present or situated within the boundaries of a state or outside the boundaries of a state, or a combination of both.

In relation to the above, state jurisdiction may be differentiated into five kinds of jurisdiction (I Wayan Parthiana, 2007):

1. Territorial Jurisdiction

   This is the jurisdiction of a state to regulate, apply, and press the national law of the state toward everything that occurs in the respective territory of the state.

2. Quasi-Territorial Jurisdiction

   It is called "quasi-territorial" because the space or place where the state jurisdiction is applied is not actually state territory, but the space or place is adjacent or connected to state territory.

3. Extraterritorial Jurisdiction

   The interests of a state are not only sufficient within its territorial boundaries or for areas nearby its territory, but may also expand to areas far removed from its territory. The interests may be in the form of legal events that involve the people (citizens) or interests of the state.

4. Universal Jurisdiction

   This is state jurisdiction that is not merely based on place, time, or actors of a legal case, but more emphasized on the universal interests of humankind.

5. Exclusive Jurisdiction

   This jurisdiction emerges because of the desire and abilities of states to explore the seafloor and the land below it, as well as to exploit its natural resources, as the consequence of progress and developments in science and technology.

In the explanation of the various jurisdictions of a state, there is the universal jurisdiction that is possessed by the state; universal jurisdiction of the state is focused on interests belonging to humankind in general. One part of the scope of the application of this jurisdiction is toward violations of human rights, which include human trafficking, genocide, and other crimes against humanity such as international terrorism and transnational crime.

As stated in the previous discussion, international terrorism is a part of crimes against humanity. This is because the characteristics of international terrorism are equivalent to those of crimes against humanity, which are actions that are inhumane and cause intense suffering toward civilians in a broad and systematic manner with political objectives.

Based on the existence of obstacles that emerge in the effort of handling the crime of international terrorism that may lead to conflict among states, international cyberterrorism should be regulated in international regulations that apply universally.

International regulations may be found in various international sources as the basis of interactions among international subjects. International treaties are the primary sources of international law that become references for international legal subjects.

International interactions in this era of globalization has continued to increase, which is marked by various cooperative agreements, including bilateral, regional, and multilateral ones. These agreements would then later on become international treaties that cover various fields and may also function as the basis for resolving problems among international legal subjects. The international treaties are the consequence of the existence of international relationships among international legal subjects.

With the application of universal jurisdiction toward the crime of cyberterrorism, it is expected that there would be agreements in definition across states as well as cooperation among states that is realized by the creation of treaties, both bilateral and multilateral ones, to handle the crime of cyberterrorism that is cross-border in nature.

IV. Conclusion

Based on the above explanation, crimes of cyberterrorism, specifically those that impact several states and threaten world security, possess similar characteristics to crimes against humanity. This is because the crime of international terrorism comprises actions that attack international interests. International terrorism is reflected by actions that attack civilians not as the objective but only as a method to fulfill the interests of the terrorist groups, and is conducted in ways that involve more than two countries, including in regard to perpetrators, victims, territories, weaponries, and funding for the activities of international terrorism. Terrorism is a crime that involves more than one state in an attack against world peace and security, whether directly or indirectly, and the handling of international terrorism is not only based on national law but also based on international law. Therefore, the crime of cyberterrorism may have universal jurisdiction applied to its handling.

Bibliography

Books

Dikdik M. Arief Mansur. (2009). Elisatris Gultom Cyber Law Aspek Hukum Teknologi Informasi, Bandung: Rafika Aditama

Dorothy E. Deninng Terror's Web: How the Internet is Transforming Terrorism, Hanbook on Internet Crime (Y. Jewkes and M. Yar, eds), Willan Publishing, 2009

Edmon Makarim, Kompilasi Hukum Telematika, Jakarta: Raja Grafindo, 2005

Erwin Asmadi, *Pembuktian Tindak Pidana Teroris (Analisa Putusan Pengadilan pada Kasus Perampokan Bank CIMB Niaga –Medan)*, Jakarta: P.T. Softmedia, 2013

Ilias Bantekas & Susan Nash;*International Criminal Law;* Cavendish Publishing; Australia;2003

Jhonny Ibrahim; *Teori & Metodologi Penelitian Hukum Normative;*Bayu Media; Malang;2007

Koalisi untuk keselamatan masyarakat sipil; *Terorisme, Definisi, dan Regulasi;* Imparsial; Jakarta;2003

Loebby Loqman, Analisis Hukum dan Perundang-Undangan Kejahatan terhadap Keamanan Negara di Indonesia, (Jakarta: Universitas Indonesia, 1990)

M.Cherif Bassiouni; *International Criminal Law;* Dobbs Ferry; New York;1986

Maskun, Kejahatan Siber (Cyber Crime) Suatu Pengantar, Jakarta: Prenada Media Grup, 2013

Richard O. Spertzel; *Iraq's Faux Capitulation;*The Asian Wall Street Journal;2002

Soeryono Soekanto, *Penelitian Hukum Normatif (Suatu Tinjauan Singkat)*, C.V Rajawali, Jakarta, 1990.

Sukarwarsini Djelantik; *Terorisme, Tinjauan Psiko-Politis, Peran Media, Kemiskinan dan Keamanan Nasional; Yayasan Pustaka Obor Indonesia; Jakarta; 2010*

Zahri Yunus dan Rabiah Ahmad, *A Dynamic Cyber-terrorism Framework dalam Internasional Journal of Computer Science and Information Security* Vol. 10, No 2, 2012.

Yasniar R.Madjid; *Konstruksi Pengaturan Kejahatan Terorisme dalam Perjanjian Internasional dengan Tanggung Jawab Integral ;* Jurnal Arena Hukum Vol 11, No 2 2018

https://arenahukum.ub.ac.id/index.php/arena/article/view/375

Journal

Ari Maharta, Made Mahartayasa; *pengaturan tindak Pidana terorisme dalam Dunia Maya (cyber Terrorism) Berdasarkan Hukum Internasional ;* Kertha Negara Jurnal Vol 04, No.06, Oktober 2016

https://ojs.unud.ac.id/index.php/Kerthanegara/article/view/24188

Nadiah Khaeriah kadir, Judhariksawan, Maskun; *Terrorism and Cyber space; A Phenomenon of Cyber-Terrorism as Transnational Crimes ;* Fiat Justicia Jurnal; Vol 13 No 4; Oktober-December 2019

https://jurnal.fh.unila.ac.id/index.php/fiat/article/view/1735

G. Grove, S. Goodman & Lukasik; *Cyber-Attacks and International Law*; Survival Global and Strategy; Vol 42; 2000-Issue 3

https://www.tandfonline.com/doi/abs/10.1093/survival/42.3.89

Edmon Makarim;*Cyber Terrorism Prevention and Eradication in Indonesia and Role and Functions of Media;* Indonesian Journal of International Law; Vol 7 No 3 Article 6; 2010

https://scholarhub.ui.ac.id/ijil/vol7/iss3/6/

Ria Anggraini Wijaya; *Kejahatan Transnasional dalam Cyber Terrorism menurut Undang-undang No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik;* Lex Crimen-eJournal Unsrat Vol 7.No 3 2018

https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/19999

Iradhati Zahra; *The Beginning of the International Humanitarian Law Application to Cyber Attack: The Status of Rule 30 Tallin Manual 1.0*; Padjajaran Journal od International Law Vol 5 No 1 Januari 2021

http://jurnal.fh.unpad.ac.id/index.php/pjil/article/view/366

B. Pratama, M.Bamatraf; *Tallin manual; cyber warfare in Indonesia Regulation*; IOP Conference Series; Earth and Environmental Science 729 April 2021

https://iopscience.iop.org/article/10.1088/1755-1315/729/1/012033

Susan W Brenner & Bert-Jaap Koops; *Approaches to Cybercrime Jurisdiction* ; Journal of High Technology Law; Vol IV No. 1 2004

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507

Xiabing Li & Yongfeng Qin; *Research on Criminal Jurisdiction of Computer Research on Criminal Jurisdiction of Computer cybercrime*; 8th International Congress of

information and Communication Technology (ICICT) 2018; Procedia Computer Science 131 (2018) 793-799

https://www.sciencedirect.com/science/article/pii/S1877050918306434

Jun Li & Jidong Jia; *Confusion and Relief of Criminal Jurisdiction of Cyber Crimes*; 3rd International Conference on Communication, Information Management and Network Security (CIMNS) 2018; Advances in Computer Science Research Vol 65 2018

https://www.atlantis-press.com/proceedings/cimns-18/25907168

I Putu Hadi Pradnyana; *Cyberterrorism Threats in Indonesia and State Responses*; Literatus Journal Vol. 2 No. 2 2020

https://journal.neolectura.com/index.php/Literatus/article/view/92

Miko Aditya Suharto; *konsep Cyber Attack, Cyber Crime dan Cyber Warfare dalam Aspek Hukum Internasional*; Risalah Hukum Vol 12 No.2 Desember 2021

https://e-journal.fh.unmul.ac.id/index.php/risalah/article/view/705

Bambang Hartono & Recca Ayu Hapsari; *Mutual Legal Assistance pada Pemberantasan Cyber Crime Lintas Yurisdiksi di Indonesia;* SASI Vol. 25 No. 1 Januari-Juni 2019

https://media.neliti.com/media/publications/315994-mutual-legal-assistance-pada-pemberantas-38412726.pdf

Dian Alan Setiawan; *Cyber Terrorism and its Prevention in Indonesia*; Media Hukum Vol. 27 No. 2 Desember 2020

https://journal.umy.ac.id/index.php/jmh/article/view/9237

Maskun, Alma Manuputy, SM.Noor & Juajir Sumardi; *Legal's Standing of Cuber Crime in International Law Contemporary;* Journal of Law, Policy and Globalization Vol 22 2014

https://www.researchgate.net/publication/315115013_Legal%27s_Standing_of_Cyber_Crime_in_International_Law_Contomperary

David P.Fidler; *Cyberspace, Terrorism and International Law;* Journal of Conflict and Security Law Vol. 21 Issue 3 Winter 2016

https://academic.oup.com/jcsl/article-abstract/21/3/475/2525373?redirectedFrom=fulltext

Nori Katagiri; *Why international law and norms do little Preventing non-state cyber attacks;* Journal of Cybersecurity Vol. 7 Issue 1 2021

https://academic.oup.com/cybersecurity/article/7/1/tyab009/6168044

Zahri Yunus dan Rabiah Ahmad, A Dynamic Cyber-terrorism Framework dalam Internasional Journal of Computer Science and Information Security Vo. 10, No 2, 2012.

Yasniar R. Madjid; *Konstruksi Pengaturan Kejahatan Terorisme dalam Perjanjian Internasional dengan Tanggung Jawab Integral;* Jurnal Arena Hukum Vol 11, No 2 2018

https://arenahukum.ub.ac.id/index.php/arena/search/authors/view?firstName=Yasniar&middleName=Rachmawati&lastName=Madjid&affiliation=Brawijaya%20University&country=ID

Yasniar R. Madjid; *Alternatif Model Penanggulangan Pendanaan Kejatan Terorisme dengan Stolen Asset Recovery;* Jurnal Jatiswara Vol 31 No 2 2016

http://jatiswara.unram.ac.id/index.php/js/article/view/43

Regulations

The Prevention of Terrorism (Temporary Provisions) act, 1984

International Convention for The Suppression of Terorist Bombing 1997

Statuta Roma Mahkamah Pidana Internasional 1998

ASEAN Convention Counter on Terrorism

United Nations Conventions Against Transnational Organized Crime (UNCATOC)

Convention of Cyber Crime

Rome Statute of the International Criminal Court 2002

Tallin manual 1.0 on the international Law Applicable to Cyber Warfare

Tallin Manual 2.0 on International Law Applicable to Cyber Operation

Internet

http;//www.angelfire.com/ca7/security/Terrirdef.html

http;//terrorism.about.com/od/whatisterroris1/ss/DefineTerrorism_4html,

http://www.scribd.com/doc/53680692/Pengertian-Cybercrime

D. E. Denning, Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. Georgetown University. 23 May 2000. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Lukasz Jachowicz, How To Prevent and Fight Internasional and Domestic Cyberterrorism and Cyberhooliganism, (warsaw: Collegium Civitas, Fpreign Policy of The United States of america, 2003), http://honey.7thguard/net/essays/cyberterrorism-policy.pdf hlm.

James A. Lewis, Assessing the Risk of Cyber-terrorism, cyber War nd Other Cyber Threats, (washington, DC: center for strategic and international studies, 2002), http://www.shaneland.co.uk/ewar/docs/dissertationsources/intitutionalsource1.pdf