Volume 13 Number 4, October-December 2019: pp. 333-344. Copyright © 2019 FIAT JUSTISIA. Faculty of Law, Lampung University, Bandarlampung, Lampung, Indonesia. ISSN: 1978-5186 | e-ISSN:2477-6238. Open Access: http://jurnal.fh.unila.ac.id/index.php/fiat

Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes

Nadiah Khaeriah Kadir
Universitas Hasanuddin, Indonesia
nadiahkhaeriah@yahoo.co.id

Judhariksawan
Universitas Hasanuddin, Indonesia
judhariksawan@gmail.com

Maskun
Universitas Hasanuddin, Indonesia
maskunlawschool@yahoo.co.id

Abstract

The advancement of information technology is changing the pattern of radical group propaganda from conventional methods to the ways they use today, namely using the media and cyberspace, or what is also called as cyber-terrorism. The purpose of this study is to discuss the emergence of the currently experienced cyber-terrorism phenomenon. It is normative research through a literature study method by approaching statutes. The results of this study indicate that cyber-terrorism is a part of cybercrime that is qualified as transnational crime which refers to Article 3 of the United Nations Convention against Transnational Organized Crime. Currently, there are several laws/regulations regarding terrorism at the national, regional and international levels. However, these rules do not specifically regulate new developments in acts of terrorism through cyberspace or what is known as cyber-terrorism.

Keywords: *Cyberspace, Terrorism, Transnational Crime.*

How to Cite: Nadiah Khaeriah Kadir, Judhariksawan, Maskun, “Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crime”, *Fiat Justisia*, 13 (4), (2019).

DOI: 10.25041/fiatjustisia.v13no4.1735

A. Introduction

The presence of Information and Communication Technology (ICT) provides convenience and excellent benefits to humans as users, namely to help solve problems in activities from simple to complex levels of difficulty, this is to achieve effectiveness and efficiency in every activity by solving problems, especially in information and communication. In ICT, there is cyberspace that is seen as a world of computer-based information and communication. In this case, cyberspace is considered as a new reality in human life which in everyday language is known as the internet.[1] Apart from the benefits gained by advancing technology in the field of computers, recent problems arise when computer networks used by various parties are miss used by certain parties for opposing interests or known as computer crime. In other terms, this crime is better known as cybercrime.[2]

One of the problems of cybercrime is the damage it can cause and gets attention from various groups that escalate into cyber-terrorism. The existence of cyberspace that is easily accessible against radicalism motivates the fast performance of such ill purpose by creating a platform. The use of cyberspace by radical organisations such as terrorists creates new threats to the international forum.

Cyber-terrorism can be understood as the convergence of terrorism and cyberspace. In this case, threats or attacks on computers where the network and information stored on it has the aim to intimidate the government and/or society for political or social purposes. Besides, to qualify as a cyber-terrorism, an attack must cause violence against people or property, or at least be harmful enough to cause fear, such as an attack that causes death or bodily injury, an explosion or significant economic loss[3].

Some terrorist groups' networks indirectly benefit from the presence of internet-based technology products that can encompass many aspects, ranging from propaganda interests, recruitment, to networking. The internet not only makes it easier for terrorists to communicate, organize terrorist cells, share information, plan attacks and recruit others but also is increasingly being used as a tool to commit acts of terrorism. Members of terrorist organisations share their knowledge through so-called online conversations where terrorists discuss various problems and plans for the future. However, these sites are

[1] Maskun, *Kejahatan Siber (Cyber Crime) Suatu Pengantar,* Jakarta: Prenada Media Group, (2013), p. 46.

[2] M. Yustia, A,“Pembuktian dalam Hukum Pidana Indonesia terhadap Cyber Crime”, *Pranata Hukum*, 5 (2), (2010), pp.77–90.

[3] Gabriela Luca,“Manifestations of Contemporary Terrorism: Cyber-terrorism”, *Research and Science Today*, 13 (1), (2017), pp. 20–25.

protected by passwords, and hence anti-terrorism analysts are often unable to access and monitor information.[4]

This cyber-terrorism act becomes a world issue that demands all countries be able to dominate the world of the internet to find out terrorist acts. The more rapid the development of new media technology, the more sophisticated the media used by terrorists and the higher the acts of terrorism can occur. Therefore, it is necessary to know the extent to which cyber-terrorism is categorized as transnational crime, given that cyberspace is borderless.

Nowadays, there are regulations relating to combating terrorism, both at the international level, namely the International Convention for the Suppression of Terrorist Bombings of New York (15 December 1997), the regional level namely the Association of Southeast Asian Nations (ASEAN) Convention on Counter-Terrorism. In the national level (Indonesia), there is Law Number 15 of 2003 on Combating Terrorism Crimes. The law allegedly occurred legal vacuum internationally, regionally and nationally to prevent and eradicate the cyber-terrorism.

B. Research Methods

This research uses a descriptive normative type of research which focuses more on literature study activities where this research is carried out by reviewing laws and regulations, books, papers, articles, journals, magazines, materials and other laws related to the object of research.[5] This study uses a statute approach with qualitative analysis by describing primary legal materials in the form of legislation and secondary legal documents in the form of research results, books, scientific journal texts, printed and electronic mass media news, and internet sites about cyber-terrorism.

C. Discussion

1. Cyber-Terrorism as Transnational Crimes

The term cyber-terrorism was first mentioned in the 1980s by Barry Collin. Collin claims that the convergence of these two worlds, virtual and physical, is the cause of cyber-terrorism. The convergence in question is cyberspace and terrorism. Cyberspace is an abstract domain and describes the virtual world where computers and networks operate, while the physical world is the place where we live. The convergence that develops from the physical

[4] Kelly Gable, "Cyber-Apocalypse Now: Securing the Internet Against Cyber-terrorism and Using Universal Jurisdiction as a Deterrent". *Vanderblit Journal of Transnational Law, 43,* (2009), pp. 57–118.

[5] Soerjono Soekanto, *Penelitian Hukum Normatif*, Jakarta: Rajawali, (2001), p. 23.

and virtual world becomes more complex and gives rise to cyber-terrorism.[6]

Professor Dorothy Denning has suggested the definition of cyber-terrorism. According to Denning, cyber-terrorism is:

"The convergence of terrorism and cyberspace. It is generally understood to mean 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.

Further, to qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact".[7]

A European Council book entitled Cyber-terrorism: The Use of the Internet for Terrorist Purposes (Terrorism and Law) defines that all activities carried out by a cell terrorist or individual over the Internet are considered cyber terrorism. In addition, The United Nations Office on Drugs and Crime classifies 6 (six) ways in which the Internet can be used for terrorist activities: propaganda deployment (recruitment, radicalisation and revolution), financing, exercise, planning (through confidential communications and open-source information), execution and cyber attacks.[8]

Cyber-terrorism or terrorism in cyberspace has been defined as the use of computers and the internet in terrorist activities. In the other hand, cyber-terrorism indeed uses computers and the internet for their activities that violate the law and to intimidate the government accordingly to achieve their goals. In this case, terrorists and the internet are closely interrelated. The internet has become a forum for terrorist groups and individual terrorists to spread messages of hatred and violence. Terrorists use encrypted email to plan the actions of internet sites of terrorist groups that reach political and social agendas.[9]

Before discussing in depth about cyber-terrorism as an international crime, it is necessary to explain what is meant by transnational crime. Transnational crime, generally defined by Passas as:

[6] Rabiah Ahmad and Zahri Yunos,"A Dynamic Cyber Terrorism Framework". *International Journal of Computer Science and Information Security*, 30 (30), (2012), pp. 149–158.

[7] Muhammad Nadjib and Hafied Cangara,"Cyber terrorism handling in Indonesia",*The Business and Management Review*, 9 (2),(2017), p. 274.

[8] Isra G. Seissa,"Cyber-terrorism Definition Patterns and Mitigation Strategies: A Literature Review". *International Journal of Science and Research (IJSR)*, 6 (1), (2017), pp. 180–186.

[9] Clay Wilson,"Computer Attack and Cyber-terrorism : Vurnerabilities and Policy Issues for Congress",https://fas.org/sgp/crs/terror/RL32114.pdf, accessed on August 1st, 2019.

"Conduct, which is criminalised in at least one of the jurisdictions concerned and jeopardises the legally protected interests in more than one of the jurisdictions concerned or in one jurisdiction while it is similar to acts which jeopardise the legally protected interests in the majority of countries."[10]

In 1995, to find out whether cyber-terrorism is indeed a part of a transnational crime, the United Nations identified several types of transnational crime: (a) money laundering, (b) terrorism, (c) theft of art and cultural objects, (d) theft of intellectual property, (e) illicit arms trafficking; (f) aircraft hijacking; (g) sea piracy; (h) insurance fraud; (i) computer crime or cybercrime; (j) environmental crime; (k) trafficking in persons; (l) human organs trade; (m) prohibited drug trafficking; (n) fraudulent bankruptcy; (o) infiltration of legal business; (p) corruption.[11]

Cyber-terrorism is a form of cybercrime. In several kinds of literature, cybercrime is often identified as computer crime. According to United States Department of Justice, computer crime described as "any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution". Another opinion proposed by Organization for Economic Cooperation Development (OECD) stipulates that use "computer-related crime" phrase means any illegal, unethical or unauthorised behaviour involving automatic data processing and/or transmission data.[12]

Cyber-terrorism is a cybercrime qualified in transnational crimes because it consists of crimes committed by terrorists cross national borders. Conceptually, transnational crime is a crime that crosses the state. This concept was first introduced internationally in the era of the 1990s at a United Nations (UN) meeting which discussed matters relating to crime prevention. On November 15, 2000 at the 62nd plenary meeting in Palermo, Italy, the United Nations adopted a convention against all forms of organised transnational crime or better known as the United Nations Convention Against Transnational Organized Crime (UNCATOC)[13].

Cyber-terrorismas transnational crimes refers to Article 3 of the United Nations Convention against Transnational Organized Crime, where the crime is: a — conducted in more than one country; b. Conducted in one country, but an essential part of preparatory, planning, directing or controlling activities

[10] Antonius Johannes Gerhardus Tijhuis, *Transnational Crime : The Interface Between Legal and Illegal Actors*, Leiden: Wolf Legal Publisher, (2006), p. 5.

[11] Basaria Panjaitan, *Mengungkap Jaringan Kejahatan Transnasional*. Bandung: Refika Aditama, (2017), p. 5.

[12] S. M. Noor, "Legal's Standing of Cyber Crime in International Law Contemporary". *Journal of Law, Policy and Globalization*, 22, (2014), p. 129.

[13] Dyah Ridhul Airin,"Kejahatan Lintas Negara Terorganisir Di Bidang Perikanan Oleh Nelayan Asing Dan Penegakan Hukumnya", *Thesis of the Faculty of Law*, Hasanuddin University, (2009).

that take place in another country; c. It is carried out in one country but involves an organised criminal group that is involved in criminal activities in more than one country; or d. Performed in one country, but has a significant effect in another.[14]

2. Motivation of Cyber-Terrorism

Social media is the main target of cyber-terrorism because of the accessibility, affordability, and broad reach of social platforms, terrorist groups use social media to realise their goals within national borders and abroad. Cyber-attacks or crimes need to have an element of terrorism (threats, harassment or violence) to be considered cyber-terrorism. There are several cyber-terrorist motives in launching the action, namely by:[15]

a. Propaganda and Psychological Warfare

The internet is used by terrorists and their organizations to spread and manage their advertisement through information warfare, to instill their ideology, to carry out psychological warfare and to radicalize and recruit new members from around the world, through terrorist websites, online magazines and various (social) media platforms (for an instance, Facebook, Twitter, Instagram, Tumblr, Vkontakte, JustPaste.it, Youtube, etc.)[16]

b. Communication and Network

Terrorist groups have used social media platforms (such as Telegram) and encrypted messaging system applications (such as Kik, SuperSpot, Wickr, Whatsapp, Gajim), online gaming chat rooms, coded or steganographic messages for confidential discussions, direct and private communication purposes (which includes networking with other group members, interactions with new members and supporters), planning and coordinating physical attacks and planning hacking operations.

c. Fundraising

Funding for terrorist-related activities (obtaining weapons or supporting war efforts by giving funds to the families of fighters) is no longer done through charitable organisations only, but it also carried out with donations through social media platforms and blogs, and the use of digital currency bitcoin.

[14] United Nations Office On Drugs And Crime,*United Nations Convention against Transnational Organized Crime and The Protocols Thereto*, (2004).

[15] A. Parlakkılıç, "Cyber Terrorism Through Social Media : A Categorical Based Preventive Approach", *International Journal of Information Security Science*, 7 (4), (2018), pp. 172–178.

[16] Mayssa Zerzri, "The Threat of Cyber Terrorism and Recommendations for Countermeasures, *Policy Advice and Strategy Development*, (04), (2017), pp. 2–3.

d. Data Mining, Recruitment and Training

Terrorists use the Internet for data mining to gather information on specific places and individuals as potential targets for attacks and recruitment. Already in the case of the September 11, 2001 attacks, Al-Qaeda used the Internet to gather and share information and then coordinate their attacks.[17]

e. The Factors of Cyber-Terrorism Approach

There are many logical reasons why terrorists are interested in using cyberspace. Their primary purpose is clearly to gain visibility and influence by creating fear by damaging infrastructure and killing people.[18] The smaller goal is to maintain its operations and carry out their activities, such as fundraising, planning, recruitment, and intelligence gathering. Terrorists use cyberspace because the cyber domain offers several benefits to achieve their goals, namely:[19]

1) Perform an anonymous communication with other terrorists;
2) Personal safety is more secure than physical attacks (for example suicide bombing missions);
3) Easy access to online data about targets;
4) Low cost (only requires a Personal Computer or smartphone);
5) Availability of many cyber-attack tools;
6) Low power: many automated attack tools require little expertise;
7) Remote access to vulnerable targets;
8) Easily reach out to network-connected targets;
9) Connections to audiences around the world for propaganda;
10) Small terrorist groups can carry out large-scale attacks.

3. A Phenomenon of Cyber-Terrorism

Cyberspace has recently emerged as the newest battleground in this digital age. The convergence of the physical and virtual world has resulted in the creation of "new threats" called cyber-terrorism. Terrorists used the Internet before the tragedy of 11 September 2001, known as the “9/11” Tragedy. Internet media is known as a potent tool for terrorist organisations. Before 1999, nearly 30 terrorist groups were found on the Internet by the United States Department of Government. However, the stronger role of the Internet for them in the aftermath of 9/11, the Al-Qaeda leadership tried to spread videos of their hiding in Pakistan through Al-Jazeera television, but

[17] *Ibid.*

[18] Giampiero Giacomello,“Bangs for the Buck: A Cost-Benefit Analysis of Cyber-terrorism”. *Studies in Conflict and Terrorism*, 27(5), (2004), pp. 387–408.

[19] *Ibid.*

they were frustrated with their very few segments so that messages could be misinterpreted which then makes them turn to the Internet to upload it more clearly and in detail without editing.[20]

In the context of the after 9/11 attacks, the threat of cyber-terrorism is often associated with Al-Qaeda and other terrorist organisations. Cyber terrorists are considered individuals who understand computers who are looking for vulnerabilities that can be easily exploited.[21] Al-Qaeda's use of the Internet is based because mass media such as television and magazines lately threaten the security of organisations and their members. The TV has limited time to broadcast great and concise news as an application of their ideology. The mass media are considered unsafe by those who allow their message to be taken by interested parties and distort the facts that affect public opinion about their actions.

Besides Al-Qaeda, the internet is also used by terrorists in Indonesia. In Indonesia itself, cyber-terrorism was detected since the 1st Bali Bombing incident on October 12, 2002. This event is considered the worst terrorist activity in Indonesia. Two years later, in 2004, the Indonesian Police succeeded in arresting the perpetrators of the site makers who were suspected of being sites used by terrorist network groups in Indonesia to carry out terrorism propaganda via the internet. From the results of the investigation it was found that Imam Samudra was executed by the Bali Bombing I bombing case (2002), apparently still had time to control the network with a set of notebooks while still being held at the Krobokan Penitentiary in Denpasar, Bali. He began to be active in cyberspace before the explosion of the Bali Bomb II in 2005, from July 2005 to being moved to Nusakambangan.[22]

4. International and National Regulations to Cyber-Terrorism

The recent rise of terrorism has raised the concerns of many States, both national and international spectrum. Terrorism leads to a loss of security in the community while also reducing the authority of the government as a body that should provide protection and security during society.[23] International, regional and national organisations have a set of laws/regulations related to terrorism. At the international level, there is the International Convention for the Suppression of Terrorist Bombings of New York, 15 December 1997. The

[20] Eska Nia Sarinastiti, “Internet Dan Terorisme : Menguatnya Aksi Global Cyber-Terrorism Melalui New Media”, *Universitas Gadjah Mada,* 1 (1), (2018), pp. 40–52.

[21] F. Cassim,“*Addressing The Spectre Of Cyber Terrorism : A Comparative Perspective”, Potchefstroom Electronic Law Journal/ Potchefstroomse Elektroniese Regsblad,* 15 (2), (2012).

[22] Ida Rochmawati, “Cyber Terorisme Dan Eksistensi Gerakan Terorisme Kelompok Islam Radikal Di Indonesia”, *INOVATIF: Jurnal Penelitian Pendidikan, Agama dan Kebudayaan,* 2 (1), (2016), pp. 33–53.

[23] Abdul Maasba Magassing, “Legal Analysis of Crime Terrorism and Counter Terrorism Strategy”, *International Journal of Advanced Research (IJAR),* 5 (7), (2017), p. 93.

convention, among others, regulates the use of explosives in public places as referred to in Article 2 : "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 is likely to result in major economic loss.[24]

Furthermore, the terror committed in the general public is explained in Article 5 : "Each State Party shall adopt such measures as may be necessary, including, where appropriate, domestic legislation, to ensure that criminal acts within the scope of this Convention, in particular where they are intended or calculated to provoke a state of terror in the general public or a group of persons or particular persons, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature and are punished by penalties consistent with their grave nature".[25]

At the regional level, there is the Association of Southeast Asian Nations (ASEAN) Convention on Counter-Terrorism. The convention regulates the prevention of terrorism as explained in Article 6: "... (b) Prevent those who finance, plan, facilitate, or commit terrorist acts from using their respective territories for those purposes against the other Parties and/or the other Parties; (c) prevent and suppress the financing of terrorist acts; (d) prevent the movement of terrorists or terrorist groups by effective border control and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents; ...(m) ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice.[26]

In addition to international and regional, there are also laws/regulations at the national level (Indonesia), namely Law Number 15 of 2003 concerning the Eradication of Terrorism Crimes. The scope of the Article on the Law on Terrorism in Indonesia is very broad, which includes the use of violence or threats that create an atmosphere of terror or widespread fear of people and cause mass casualties. Likewise, actions that result in damage to vital strategic objects, as regulated in Article 6 to Article 17 with the threat of imprisonment

[24] United Nations General Assembly, *International Convention for the Suppression of Terrorist Bombings,* (1997).
[25] *Ibid.*
[26] Association of Southeast Asian Nations, *ASEAN Convention On Counter Terrorism,* (1976).

of at least three years until the death sentence.[27]

From the conventions and laws mentioned above, can meet the needs of combating terrorism in general. However, it has not yet accommodated new developments in the cyber world with features anonymity, borderless, mobility.[28]

D. Conclusion

Cyber-terrorism is one of the cybercrimes that is qualified as transnational crimes because the crimes are committed by terrorists that cross national borders. Currently, there are several laws/regulations regarding terrorism at the national, regional and international levels. However, these rules do not specifically regulate new developments in acts of terrorism through cyberspace or what is known as cyber-terrorism. Therefore, the current law and regulation cannot be used to overcome the problem of cyber-terrorism. As a recommendation, it is essential to include the substance of cyber-terrorism in the legislation governing the issue of terrorism because cyber-terrorism including transnational crime that can threaten the country, both nationally and internationally.

Bibliography

A. Books

Maskun. (2013). *Kejahatan Siber (Cyber Crime) Suatu Pengantar.* Jakarta : Prenada Media Group.

Panjaitan, Basaria. (2017). *Mengungkap Jaringan Kejahatan Transnasional*. Bandung: Refika Aditama.

Soekanto, Soerjono. (2001). *Penelitian Hukum Normatif*. Jakarta: Rajawali.

Tijhuis, Antonius Johannes Gerhardus. (2006). *Transnational Crime : The Interface Between Legal and Illegal Actors*. Leiden: Wolf Legal Publisher.

B. Journals

A. Parlakkılıç, “Cyber Terrorism Through Social Media : A Categorical Based Preventive Approach”, *International Journal of Information Security Science*, 7 (4), (2018), pp. 172–178.

Abdul Maasba Magassing, “Legal Analysis of Crime Terrorism and Counter Terrorism Strategy”, *International Journal of Advanced Research (IJAR),* 5(7), (2017), p. 93.

Eska Nia Sarinastiti, “Internet Dan Terorisme: Menguatnya Aksi Global

[27] Peraturan Pemerintah Pengganti Undang-Undang Republik Indonesia Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme.

[28] Afitrahim,“Yurisdiksi Dan Transfer Of Proceeding Dalam Kasus Cybercrime”, *Thesis of the Faculty of Law,* University of Indonesia, (2012).

Cyber-Terrorism Melalui New Media", *Jurnal Gama Societa*, 1(1), (2018), pp. 40–52.

F. Cassim, "Addressing The Spectre Of Cyber Terrorism : A Comparative Perspective", *Potchefstroom Electronic Law Journal Potchefstrooms eElektroniese Regsblad,* 15 (2), (2012), https://doi.org/10.4314/pelj.v15i2.14.

Gabriela Luca, "Manifestations of Contemporary Terrorism: Cyber-terrorism", *Research and Science Today*, 13 (1), (2017), pp. 20–25.

Giampiero Giacomello, "Bangs for the Buck: A Cost-Benefit Analysis of Cyber-terrorism", *Studies in Conflict and Terrorism*, 27 (5), (2004), pp. 387–408, https://doi.org/10.1080/10576100490483660.

Ida Rochmawati, "Cyber Terorisme Dan Eksistensi Gerakan Terorisme Kelompok Islam Radikal Di Indonesia". *INOVATIF: Jurnal Penelitian Pendidikan, Agama Dan Kebudayaan,* 2 (1), (2016), pp. 33–53.

Isra G. Seissa,"Cyber-terrorism Definition Patterns and Mitigation Strategies: A Literature Review", *International Journal of Science and Research (IJSR),* 6 (1), (2017), pp. 180–186. https://doi.org/10.21275/art20163936.

Kelly Gable, "Cyber-Apocalypse Now: Securing the Internet Against Cyber-terrorism and Using Universal Jurisdiction as a Deterrent". *Vanderblit Journal of Transnational Law,* 43, (2009), pp. 57–118, https://doi.org/10.2139/ssrn.1452803.

M. Yustia A,"Pembuktian dalam Hukum Pidana Indonesia terhadap CyberCrime", *Pranata Hukum*, 5(2),(2010), pp.77–90.

Mayssa Zerzri, "The Threat of Cyber Terrorism and Recommendations for Countermeasures", *Policy Advice and Strategy Development,* (04), (2017), pp. 2–3.

Muhammad Nadjib and Hafied Cangara, "Cyber terrorism handling in Indonesia", *The Business and Management Review*, 9 (2), (2017), p. 274.

Noor, S. M, "Legal's Standing of Cyber Crime in International Law Contemporary". *Journal of Law, Policy and Globalization,* 22, (2014), p. 129.

Rabiah Ahmad and Zahri Yunos, "A Dynamic Cyber Terrorism Framework". *International Journal of Computer Science and Information Security*, 30 (30), (2012), pp. 149–158.

C. Legislations

Association of Southeast Asian Nations, *ASEAN Convention On Counter Terrorism,* (1976).

Peraturan Pemerintah Pengganti Undang-Undang Republik Indonesia Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme.

United Nations General Assembly, *International Convention for the Suppression of Terrorist Bombings,* (1997).

United Nations Office On Drugs And Crime, *United Nations Convention against Transnational Organized Crime and The Protocols There to*, (2004).

D. Internet and Thesis

Afitrahim, *Yurisdiksi Dan Transfer Of Proceeding Dalam Kasus Cybercrime,* Tesis Fakultas Hukum Universitas Indonesia, (2012).

Clay Wilson,"Computer Attack and Cyber-terrorism: Vurnerabilities and Policy Issues for Congress", https://fas.org/sgp/crs/terror/RL32114.pdf, accessed on August 1st, 2019.

Dyah Ridhul Airin,*Kejahatan Lintas Negara Terorganisir Di Bidang Perikanan Oleh Nelayan Asing Dan Penegakan Hukumnya*, Tesis Fakultas Hukum Universitas Hasanuddin, (2009).