

Cyber Terrorism Criminal Acts in the Perspective of Transnational Organized Crime



Okti Putri Andini

Postgraduate Program, Faculty of Law, Universitas Diponegoro
Semarang, Indonesia

 oktiputri30@gmail.com

ARTICLE INFORMATION

History of Article

Submitted : 17 May, 2021
Revised : July 23, 2021
Accepted : September 21, 2021

Copyrights



Copyrights is on Author(s), and publishing rights on Publisher. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Conflicting Interest Statement

All authors declared that there is no potential conflict of interest on publishing this article.

Funding

None

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Cite this article as:

Andini, O. P. (2021). Cyber Terrorism Criminal Acts in the Perspective of Transnational Organized Crime. *Unnes Law Journal: Jurnal Hukum Universitas Negeri Semarang*, 7(2), 333-346. <https://doi.org/10.15294/ulj.v7i1.38804>

Cyber Terrorism Criminal Acts in the Perspective of Transnational Organized Crime

Okti Putri Andini

ABSTRACT. This research was conducted to explain the legal instrument governing Cyber terrorism from an organized transnational crime perspective as well as analyzing the modus operandi used by Cyber terrorism. This research is normative legal research using a qualitative approach to finding data sources by studying all the laws and regulations concerned with Cyber terrorism. Because this research is normative legal research then the data sources used in this research are secondary data sources. In collecting data, authors conduct literature studies, and the validity of the obtained data is examined using triangulation techniques. Then the results are analyzed and presented using a descriptive analytical method. The results of this study found that there were several international conventions that could be used as legal instruments for Cyber terrorism. And based on the study by the authors modus operandi used by terrorists in committing Cyber terrorism very diverse namely through hacking, propaganda, fraud, DDoS attacks and the spread of viruses, worms or malware. The outcome of the results are although there is no legal instrument that governs Cyber terrorism but some of the relevant and existing international conventions can be used as Cyber terrorism law resource, and it can be noted that there are various of modus operandi used by terrorists in Cyber terrorism.

KEYWORDS. Cyber terrorism; Organized Transnational Crime; International Criminal Law

Cyber Terrorism Criminal Acts in the Perspective of Transnational Organized Crime

Okti Putri Andini

Introduction

The development of information technology today is very broad and without limits, behind all the positive sides that can be utilized the development of information technology also shows the negative side. The crimes caused by the internet are currently reaching international and transnational dimensions. One crime that is related to the internet and has a transnational dimension is a crime that we can call Cybercrime or crime through the internet network. The Encyclopedia of Cybercrime divides Cybercrime crime into several types and one of them is *Cyber terrorism*. *Cyber terrorism* is a crime undertaken by persons who intend to advance social, religious or political objectives but by causing widespread fear or by damaging or disrupting important infrastructure information.¹

According to the United Nations Office on Drugs and Crime (UNODC) in its research as many as 7% of UNODC member countries agreed that Cyber terrorism is one crime that is considered to have a significant effect of damage if it befalls a country. According to the data collected by the author,

¹ Samuel C. McQuade, Encyclopedia of Cybercrime, USA: Greenwood Press The Concise Oxford Dictionary of Current English (8th edition) 1990, (Oxford: Clarendon Press, 2009), p. 44

since 1996 up to 2019 there have been approximately 17 cases in the world which are one form of cyber terrorism in various ways and targets. However, the high number of cyber terrorism has not been matched up to now with special regulations that can be used to deal with cyber terrorism crimes globally. Though establishing a global legal basis to fight Cyber terrorism is very important.².

The importance of regulations regarding Cyber terrorism is not only due to the absence of specific regulations governing these criminal acts, but also because of the position of cyber terrorism crimes which is one form of organized transnational crime. The determination was concluded because of the borderless nature of the cyber terrorism crime which makes the scope of the crime will be very broad because it involves more than one country, as well as between victims and perpetrators of crime can be from different countries which results in differences in the jurisdiction of cyber-criminal law enforcement. terrorism.

Various forms of criminal acts that are used as a *modus operandi* used by terrorists in committing criminal acts of Cyber terrorism are also one of the reasons why there is a need for special regulations for the enforcement of Cyber terrorism criminal acts. One of the methods or *modus operandi* used by terrorists in committing cyber terrorism is the spread of propaganda, national law and international law do not yet regulate the crime of spreading propaganda. If regulations regarding one form of cyber terrorism are not yet available, it will be difficult for a country in terms of law enforcement efforts.

The high rate of implementation and the wide scope of cases of Cyber terrorism, which is one form of organized transnational crime, makes arrangements that regulate Cyberterrorism criminal acts really needed. Therefore, the writer wants to examine this Cyber terrorism crime from the perspective of organized transnational crime, so that it can explain the legal instruments that can be the basis of law enforcement for Cyber terrorism crime, and find the *modus operandi* carried out by terrorists in launching acts of terror.

The theory of policy or politics of criminal law is one of the theories used by the author as a basis for this research. The purpose of this research is in line with efforts to carry out criminal law policies or politics.

² Enver Bucaj, *The Need for Regulation of Cyber Terrorism Phenomena in Line with Principles of International Criminal Law*, *Juridica*: Vol 13 No 17, (Galati: Universitatea Danubius, 2017), p. 160

CYBER TERRORISM CRIMINAL ACTS

International Criminal Law, Global Security Studies

Implementing criminal law politics means that we are holding an election to create good results in formulating a law, a good law.³ Here it means that the meaning of the implementation of the politics of criminal law is how to maximize in terms of the making and formulation of a law or law in order to be carried out maximally and produce fair results. And aims to protect the community in order to achieve community welfare⁴

Pre-existing related research is also a reference in carrying out this research. The first study is titled "*Analysis of Cyber Terrorism Instruments in the Framework of the International Law System*" by Alfira Nurliliani Samad, Hasanudin University Makasar. The results of the study conclude that the crime of Cyber terrorism is not included in international crimes but included in the form of transnational crime. It was concluded that although there is no juridical regulation in international law that regulates cyber crime, there are a number of international conventions that can be used as a reference for legal sources for handling cyber terrorism crimes.

Research titled "Arrangement of Criminal Acts of Terrorism in the Cyber World (Cyber terrorism) Based on International Law". By Ari Maharta, Udayana University, Bali also stated the same thing that cyber terrorism is categorized as one of the categories of organized transnational crime not as a form of international crime and there is not yet any international legal instrument that specifically regulates cyber terrorism but in order to fill the legal vacuum, the ASEAN Convention on Counter Terrorism and the International Convention for the Suppression of Terrorist Bombings can be used temporarily.

Method

This research is normative legal research using a qualitative approach in finding data sources by examining all relevant laws and regulations related to cyber terrorism. Because this research is normative legal research, the source of the data used in this study is a secondary data source with three different legal materials. In collecting data, the authors conducted a literature study and the validity of the data obtained was examined using triangulation

³ Sudarto, Law and Criminal Law, (Bandung: Alumni, 1981), p. 159

⁴ Barda Nawawi Arief, Interest in Criminal Law Policy. (Jakarta: Prenadamedia Group, 2008), p. 28

techniques. Then the results are analyzed and presented using descriptive analytical methods.

Cyber terrorism as part of Cybercrime, Terrorism and Transnational Crime

The term cyber terrorism has been applied by several people to describe the use of the internet for terrorist purposes⁵(Jarvis, 2015: 69). Cyber terrorism is a special type of terrorism, where the "place" or "media" used is virtual space (Mayer, 2018). Cyber terrorism is a crime that involves the use of computer systems to carry out terrorist acts. Cyber terrorism is basically characterized by threats or destruction on a large scale, coupled with the intention to injure or pressure society or the government of a country (Whiting, 2018: 6). In other words, we can know that Cyber terrorism emerged as a new type of terrorism. The method of terrorism is carried out in cyberspace or cyberspace. But the results are really real and destructive⁶ (Terzi, 2019: 229).

Based on the definition of Cyber terrorism, it can be seen the elements contained in Cyber terrorism, including:

- 1) The crime uses the technology media, precisely the computer system.
- 2) The main action of the goal of Cyber terrorism itself is to carry out terrorism. The culprit is a terrorist, a group or organization.
- 3) Forms of crime in the form of threats or destruction of computer systems that cause large-scale damage.
- 4) The impact of these crimes can be physical attacks in the form of injuring or suppressing (causing fear) the community or government of a country.
- 5) This crime can be committed anywhere, between different countries.

The elements of Cyber terrorism above indicate that such crimes are part of Cybercrime and terrorism is also part of Transnational Crimes. This is indicated by the compatibility between the elements of cyber terrorism and the qualification of transnational crime contained in Article 3 of the United Nations Convention against Transnational Organized Crime (United Nations

⁵ Lee Jarvis, Samuel Macdonald, What is Cyber terrorism? Finding From Survey of Researchers, *Journal of Terrorism and Political Violence*: Vol 27 Issue 4, 2015, p. 69

⁶ Mahir Terzi, *Turkish Journal of TESAM Academy: E-Government and Cyber terrorism: Conceptual Framework, Theoretical Discussions and Possible Solutions*. (Turkey: TESAM Academy Dergisi, 2019) p. 229

CYBER TERRORISM CRIMINAL ACTS

International Criminal Law, Global Security Studies

Convention against Transnational Organized Crime), stating that a crime can be called Transnational Crime if :

- 1) Conducted in more than one country;
- 2) Conducted in one country but an important part of the preparation, planning, direction or control activities occur in another country;
- 3) It is carried out in one country but involves an organized criminal group that is involved in criminal activity in more than one country; or
- 4) It is carried out in one country but has major consequences in another.

This classification matches the elements of Cyber terrorism because based on the elements of Cyber terrorism above it is known that Cyber terrorism is not limited by geographical boundaries, because their actions occur in the virtual world so that it can be done remotely and from anywhere in the world which of course conducted in more than one country.

Cyberterrorism Criminal Procedure Instrument

- 1) Law Number 19 Year 2016 concerning Amendments to Law Number 11 Year 2008 concerning Information and Electronic Transactions.
- 2) Law Number 5 of 2018 concerning Amendment to Law Number 15 of 2003 concerning Eradication of Terrorism Crimes.
- 3) 2000 United Nations Convention against Transnational Organized Crime (2000).
- 4) Budapest Convention (Convention on Cybercrime) 2001
- 5) The 1997 International Convention on the Suppression of Terrorist Bombings

The modus operandi of cyber terrorism

ISIS is a pioneer in deploying Cyber terrorism. This statement comes from the fact that these extremist organizations use Cyberspace more intensively and systematically. ISIS first appeared in 2013 under the leadership of Abu Bakr al-Baghdadi. ISIS is involved in "new terrorism" where computers and the internet take an important role in terrorism. This new media of terrorism expands ISIS activities in Cyberspace, especially realizing the ISIS goal not to cause death, but to create terror and insecurity in society. ISIS is a real threat to Cyberspace, because it recruits many

experienced hackers with the computational skills needed to hack into the system and destroy the target computer.⁷ (Lilington, 2016).

ISIS takes jihad to new ways and levels. Cyberspace is a tool used by ISIS to target Jihadists. ISIS recruits and radicalizes new members and instils their beliefs and ideology of jihad in Jihadists. In addition, ISIS also promotes "lone wolf" attacks through social media, inviting supporters to fight against targets⁸. In committing the crime of Hybrid Cyber terrorism ISIS uses hacking, propaganda, and fraud under the guise of charity as its mode of operation.

Hacking

Hacking activities can include the act of using hardware or wrong software implementation to obtain passwords illegally to gain access to a computer system⁹. Hacking actions one of which was carried out by ISIS supporters and several hacker teams that are closely related to ISIS and who support the objectives of ISIS by launching Cyber-attacks, they are:

Cyber Caliphate Army (CCA) was one of the first Cyberterrorist groups to support ISIS. CCA has carried out significant Cyberterrorist attacks in 2015, the most influential CCA Cyberterrorist attacks in the world of Cybercrime are attacks on the United States Central Command Twitter and YouTube accounts and also the Twitter accounts of Newsweek magazine¹⁰.

Sons Caliphate Army was established in February 2016, SCA has claimed that they are the culprits behind 15,000 attacks on Twitter and Facebook accounts worldwide. The SCA also claims to have hacked the website of the Central Bank of Bangladesh, SCA claims responsibility for the hacking case of the Arabic site of the English football club Arsenal and distributed anti-Shi'a videos as a form of propaganda¹¹

United Cyber Caliphate (UCC) is a coordinated party and plays an important role in ISIS Cyber terrorism. The group was created in May 2016 by a combination of three hacker groups namely the Cyber Caliphate Army,

⁷ Karlin Lillington, How Real Is The Treat of Cyberterrorism ?, Irish Times, 2016

⁸ Dominika Gintas, Dimitrios Stergiou, *From Terrorism to Cyber terrorism: The Case of ISIS*, (Greece: 2018) p. 9

⁹ Marcus Ayodeji Arraromi, Cyber-terrorism under the Nigerian law: a new form of threat or an old threat in a new skin ?, (Nigeria: 2018), p. 11

¹⁰ Lait Alkhouri, et.all, *Hacking for ISIS*. (Falshpoint Publisher: 2016) p. 4

¹¹ Alkhouri, *Ibid*, p. 15

CYBER TERRORISM CRIMINAL ACTS

International Criminal Law, Global Security Studies

the Kalashnikov E-Security Team, and the Sons Caliphate Army. The main activity of the UCC is to publish a "kill list" in the telegram.

Islamic Cyber Army. This hacker group stated that it would carry out a cyber attack on the 9/11 anniversary. As a result, these actions create fear and strengthen the insecurity of Americans for the possibility of a repeat of terrorist attacks in America. On September 11 the group began to reveal the start of the attack by announcing on Twitter that they had hacked the White House's name, address and telephone number.

Islamic Cyber Army also held a discussion with Amrah Bank, one of the most important and most important banks of Azerbaijan. ICA hackers damaged the Amrah Bank website by placing ISIS flags, ICA logos, photos of Osama bin Laden and the World Trade Center. The Amrah Bank attack was one of the cyber attacks that directly affected the life of the economy of Azerbaijan, the impact of which was almost the same as traditional terrorism in general.¹².

Propaganda

Terrorists and terrorist organizations spread and manage their propaganda through information warfare, to convey their ideology, to wage war and to radicalize and recruit new members from around the world, through terrorist websites, online magazines, and various social media platforms such as Facebook, Twitter, Instagram, Tumblr, and Youtube¹³.

Internet propaganda can also include content such as video recordings of cruel acts of terrorism or video games developed by terrorist organizations that simulate acts of terrorism and encourage users to engage in role playing by acting as part of virtual terrorists. An example is a video game titled "Salil al Sawarem" (The Clanging of the Swords), owned by ISIS. Other objectives of terrorist propaganda can include the use of psychological manipulation to undermine an individual's beliefs in certain social values, or spread an increased sense of anxiety, fear or panic among citizens¹⁴. Examples of

¹² Giantas, Op.Cit, p. 18

¹³ Mayssa Zerzri, The Threat of Cyber Terrorism and Recommendations for Countermeasures. No 4. CA Perspective on Tunisia, (Tunisia: 2017), p. 2

¹⁴ Ahmed Al-Rawi, Video games, terrorism, and ISIS's Jihad 3.0, Terrorism and political violence journal: Vol. 30 No.4, DOI: 10. 1080 / 09546553.2016.1207633, 2018, p. 740

terrorist propaganda in cyberspace are actions carried out by the following groups:

Kalashnikov E-Security Team is a hacking group founded in 2016. In terms of helping ISIS propaganda, the group also makes and uploads literature related to ISIS jihad, distributes posts belonging to the Cyber Caliphate group, reports the success of attacks carried out on websites and Facebook pages and publishes a variety of ways or web hacking techniques.

The group Rabitat Al-Ansar is a group whose role is to spread the ideology of jihadism and recruit new members of ISIS, by publishing articles, praising ISIS and the ideology of jihad, distributing the daily news of the Islamic world and the victory of ISIS to people considered "unbelievers" to participate in his class¹⁵.

Computer Based Fraud

In the world of modern electronic banking fundraising can be achieved directly or indirectly, either through legal or illegal transitions. The ways in which terrorists use the internet to collect funds and resources can be classified into four general categories, namely in the form of direct requests, e-commerce, exploitation of online payment instruments and fraud through online charity organizations.

Online payment facilities are exploited through fraudulent means such as identity theft, credit card theft, fraud, intellectual property crime and auctions. Like the use of Paypal financial technology facilities by terrorists¹⁶.

Funding through online charity organizations allows donors to not realize that the funds that donors provide are used for terrorist organizations. Because fundraising is fundraising under fake charities that indicate donations will be used for humanitarian purposes. For example, the formation of charities for disaster relief, such as the devastating earthquake in Pakistan in 2005. While the charity has undertaken several aid projects, some of the proceeds are channeled to terrorist organizations. These 'charities' can be easily established by terrorist supporters and cannot be distinguished from actual fundraising¹⁷.

¹⁵ Alkhouri, Op.Cit, p. 13

¹⁶ UNODC, *The Use of the Internet for Terrorist Purpose*, (New York: United Nations, 2012) p. 17

¹⁷ Major Charvat, *The Virtual Battlefield: Perspectives on Cyber Warfare: Cyber terrorism: A new Dimension in Battlespace*. (IOS Press, 2009), p. 83

CYBER TERRORISM CRIMINAL ACTS

International Criminal Law, Global Security Studies

Funding for terrorist-related activities is no longer only done through charitable organizations. In exchange for donations through the media platform and blog, as well as the use of the digital currency bitcoin also becomes a media for terrorist funding. For example, Indonesian security forces found financial transfers made by an ISIS operator to Indonesian terrorists (Bahrul Naim) using the digital currency bitcoin¹⁸.

DDoS attack (Denial Distributed of Service)

Distributed Denial of Service (DDoS) also known as an overload attack is an attack launched online, involving bombarding IP addresses with large amounts of data traffic, causing the main homepage in online services or network components to be overloaded, making it unusable for users. Potential targets for DDoS attacks are chat and mail servers, government websites, high-volume sites such as search engines, e-commerce sites, and news services.

One example of DDoS attacks carried out by terrorists is DDoS attacks carried out by ISIS's Cyber Caliphate Army, the group used DDoS attacks successfully against Yemen and Iraqi government sites in January 2017, resulting in government sites having to be offline for two months¹⁹(Stroobants, 2018: 77). Hackers of terrorist organization sympathizers also plan and carry out DDoS attacks with the aim of attracting the attention of terrorist organizations and their aim as part of an intimidation campaign against civilians.

Malware Attack

Malware (or malicious software) is software code that, when spread, is designed to infect, change, destroy, delete or replace data or information systems without the owner's knowledge or consent. Malware includes computer viruses, worms, botnets, Trojan horses, phishing tools, spyware tools, and other malicious and unwanted software.²⁰(Ambrosio, 2015: 12).

¹⁸ Zerzri, Op.Cit, p. 3

¹⁹ Serge Stroobants, Expert Contributions: Cyberterrorism is The New Frontier, (Global Terrorism Index: 2018), p. 77

²⁰ Ponciano Jorge Escamilla Ambrosio, Cyber security A-15, (Mexico: National Polytechnic Institute, 2015) p. 12

The malware can bring down the system and network which causes a large disturbance to the target. This can make important operating systems temporarily unusable or make them unable to function²¹ (Araromi, 2018: 12).

Malware attacks that have occurred, one of which is the WannaCry Ransomware Virus Attack in 2017, Cyber attacks carried out by terrorist groups that use NSA hackers, attacking institutions in 99 countries including Britain, the United States, China, Russia, Spain, Italy and Indonesia . The institutions which were the target of the attack were hospitals, universities and government sites. In Indonesia WannaCry's ransomware attacked two major hospitals in Jakarta which caused paralysis of the hospital's information network and stopped hospital services for a while.

Conclusion

Cyber terrorism is part of Cybercrime and criminal acts of terrorism. And considering the borderless nature of Cyber terrorism, Cyber terrorism can be categorized as a transnational crime. The unavailability of legal instruments for criminal acts of Cyber terrorism can be covered by several national and international legal instruments whose regulations are in accordance with Cyber terrorism criminal acts, namely Law Number 19 Year 2016 concerning Amendments to Law Number 11 Year 2008 concerning Information and Electronic Transactions, and Law Number 5 Year 2018 concerning Amendment to Law Number 15 Year 2003 concerning Eradication of Terrorism Crimes. And according to international criminal law, there are several international conventions that can be used as legal instruments regulating the crime of Cyber terrorism. These international conventions are the United Nations Convention against Transnational Organized Crime Palermo, Italy in 2000; Budapest Convention on Cybercrime 2001; and the International Convention for the Suppression of Terrorist Bombing in New York, United States of America in 1998. Furthermore, terrorists in committing criminal acts of Cyber terrorism have different *modus operandi*. Because the internet can be exploited easily, terrorist organizations have various ways to carry out these crimes. Terrorist organizations like ISIS use the internet to help them realize their goals. ISIS creates and utilizes hacking organizations to facilitate them in committing the

²¹ Araromi, Op.Cit, p. 12

CYBER TERRORISM CRIMINAL ACTS

International Criminal Law, Global Security Studies

crime of Cyber terrorism. ISIS is assisted by the Cyber Caliphate Army (CCA); Sons Caliphate Army (SCA) Kalashnikov E-Security Team; United Cyber Caliphate; The Islamic State Hacking Division (ISHD); Islamic Cyber Army (ICA); The group Rabitat AL-Ansar; and the Cyber Rox Team (CTR). Based on various activities carried out by the hacking organization, the modus operandi used by ISIS in committing cyber terrorism is to carry out cyber attacks in the form of hacking, propaganda, fraud in order to obtain funding, Distributed Denial of Service (DDoS) attacks and Malware attacks.

References

- Alkhouri, L. Kassirer, A. and Nixon, A. 2016. Hacking for ISIS. Falshpoint Publisher
- Al-Rawi, A. 2018. Video games, terrorism, and ISIS's Jihad 3.0. Terrorism and political violence journal: Vol. 30 No.4. DOI: 10. 1080 / 09546553.2016.1207633
- Ambrosio, PJ E. 2015. Cyber security A-15. Mexico: National Polytechnic Institute
- Arief, Barda N. 2008. Interest in Criminal Law Policy. Jakarta: Prenadamedia Group
- Arraromi, M. Ayodeji. 2018. Cyber-terrorism under the Nigerian law: a new form of threat or an old threat in a new skin ?. Nigeria.
- Bucaj, E. 2017. The Need for Regulation of Cyber Terrorism Phenomena in Line With Principles of International Criminal Law. Juridica: Vol 13 No 17. Galati: Universitatea Danubius.
- Charvat, M. 2009. The Virtual Battlefield: Perspectives on Cyber Warfare: Cyber terrorism: A new Dimension in Battlespace. IOS Press
- Giantas, D. Stergiou, D. 2018. From Terrorism to Cyber terrorism: The Case of ISIS. Greece.
- Jarvis, L. Macdonald, S. 2015. What is Cyber terrorism? Finding From Survey of Researchers. Journal of Terrorism and Political Violence: Vol 27 Issue 4.
- Lillington, K. 2016. How Real Is The Treat of Cyberterrorism ?. Irish Times
- McQuade, SC 2009. Encyclopedia of Cybercrime. USA: Greenwood Press
- The Concise Oxford Dictionary of Current English (8th edition). 1990. Oxford: Clarendon Press

- Stroobants, S. 2018. Expert Contributions: Cyberterrorism is The New Frontier. Global Terrorism Index
- Sudarto. 1981. Law and Criminal Law. Bandung: Alumni.
- Terzi, M. 2019. Turkish Journal of TESAM Academy: E-Government and Cyber terrorism: Conceptual Framework, Theoretical Discussions and Possible Solutions. TESAM Academy Dergisi.
- UNODC. 2012. The Use of Internet For Terrorist Purpose. New York: United Nations
- Whiting, A. Macdonald, S. Jarvis, L. 2018. Cyber terrorism: Understandings, Debates and Representations. Accessed at <https://www.cambridge.org> at 14/01/20 2019
- Zerzri, M. 2017. The Threat of Cyber Terrorism and Recommendations for Countermeasures. No 4. CA Perspective on Tunisia