Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10183568

CRIMINAL LAW POLICY IN HANDLING CYBER TERRORISM AS A FORM OF CYBERCRIME IN INDONESIA

BUDIONO SANDI *

Student of Doctoral Program in Law, Faculty of Law, Diponegoro University, Jl. Prof. Soedarto, SH., Tembalang, Semarang, Indonesia. *Corresponding Author Email: budionosandi@students.undip.ac.id

RETNO SARASWATI

Lecturer of Doctor of Law Program, Faculty of Law, Diponegoro University, Jl. Prof. Soedarto, SH., Tembalang, Semarang, Indonesia.

ANI PURWANTI

Lecturer of Doctor of Law Program, Faculty of Law, Diponegoro University, Jl. Prof. Soedarto, SH., Tembalang, Semarang, Indonesia.

Abstract

This study aims to analyze the criminal law policy in dealing with criminal cyberterrorism as a form of cyberterrorism crime. The method used is normative juridical. The results showed that cyberterrorism is a form of terror transformation carried out by terrorists by making the internet network as a tool or target of attack. Criminal law policy in Indonesia has two legal instruments that can be used as a source of law enforcement of cyber terrorism, namely Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, and Law Number 5 of 2018 concerning Amendments to Law Number 15 of 2003 concerning Eradication of Criminal Acts of Terrorism. And according to international criminal law, there are several international conventions that can be used as legal instruments to regulate cyber terrorism. These international conventions are the United Nations Convention against Transnational Organized Crime Palermo, Italy in 2000; The Budapest Convention on Cybercrime 2001; and the International Convention for the Suppression of Terrorist Bombing New York, United States in 1998.

Keywords: Criminal Law, Policy, Criminal Acts, Cyberterrorism, Cybercrime.

A. INTRODUCTION

The development of information technology today is very broad and boundless, behind all the positive sides that can be utilized the development of information technology also shows negative sides (Sari et al., 2020). The crimes caused by the internet are now reaching an international and transnational dimension. The term international crime itself refers to a criminal event of an international nature (Sadino & Dewi, 2021).

The international definition in this case is the understanding in a broad sense, including, general or global international, regional or bilateral and trilateral (Nadu, 2017). In other words, the crime can concern the interests of all or most countries in the world, even the interests of all mankind can also be only the interests of the country or region, or only concern the interests of two or more countries (Maqableh et al., 2021).

In addition, crimes caused by the internet can also have transnational dimensions which are commonly referred to as transnational crimes. Crimes are crimes that are essentially

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10183568

national dimensions but have transnational or transnational characteristics (Zakaria, 2012).

The locus delicti of transnational crime is in fact still within the boundaries of a country's territory, but in its execution transnational crime involves the affairs of other states, so that it seems as if there are two or more states that have an interest in the crime. So the real point of transnational crime is that it is of dimensionals, but because of the connection with the interests of other countries, it seems to be transnational in nature (Anggraeni & Rizal, 2019).

One of the crimes related to the internet and has a transnational dimension is a crime that we can call cybercrime or crime through the internet network (Gani & Gani, 2019). According to the Ministry of Foreign Affairs of the Republic of Indonesia, Cybercrime is included in the category of transnational crimes, considering that one of the special characteristics of Cybercrime crimes is that these crimes are committed online and are often not clearly linked to any geographical location, so they often go beyond the borders of other countries. And one of the hallmarks of transnational crime is that it is committed beyond national borders, so this Cybercrime already qualifies as one of the parts of transnational crime (Ismoyo, 2014).

In addition to these reasons, in 2010 the Conference of States Parties (CoSP) of the United Nation Convention Against Transnational Organized Crime (UNTOC) mentioned that there are several new crimes identified as New and Emerging Crimes, these crimes include cybercrime, identity-related crimes, illicit sale of cultural heritage, environmental crimes, piracy. above the sea, and the illicit trade of body organs (Martin & Romano, 1992). New Transnational Crimes are currently given special attention by the international world because the number of crimes is quite high, the losses caused are large and the modus operandi used is also very diverse (Sitompul, 2012).

Cybercrime is a criminal attack that involves or occurs on Cyberspace, a very subtle region created when computers and 3 people are connected through an electronic network that spans the entire world. Cybercrime, which has emerged as a crime issue and international courts, is the downside of the influx of digital communication technologies, especially the internet, into everyday life and global trade (Vilic, 2017).

The notion of Cybercrime is evolving linearly with the development of crime on the internet. In the beginning, Cybercrime only included computer crime, which is a crime targeted at a computer or computer used as a tool to commit crimes. But currently the scope of Cybercrime includes a more varied and broad range of crimes, not only forms of computer crime but also other forms of crime including computer related crime (Theohary & Rollins, 2015).

The Encyclopedia of Cybercrime divides Cybercrime crimes in several types and one of them is Cyber terrorism (Rapporteur, 2010). In the Encyclopedia of cybercrime it is said that: "Cybercrime is a term that encompasses all the ways by which computers and other types of portable electronic devices such as mobile phones and PDAs capable of connecting to the internet are used to break the law and cause harm" (ITU, 2009).

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10183568

Cyber terrorism is a crime committed by individuals who intend to promote social, religious or political purposes but by causing widespread fear or by damaging or disrupting critical infrastructure information. Based on the explanation of the types of Cybercrime, Cyber terrorism is an emerging crime (Bobic, 2014). This crime uses the media of 4 computers in spreading terror ideologies to carry out terrorist crimes on the internet. The Internet mentions the term Cyber terrorism as an activity where a group of terrorists uses Cyberspace media to carry out acts of terrorism. So Cyber terrorism itself consists of elements of Cyberspace and terrorism (Ardiyanti, 2016).

The definition of Cyberspace is not limited to the world created as a result of relationships through the internet. The internet can spread information quickly with little risk, and does not require expensive costs to recruit potential, making it easy to potentially acquire prospective partners in terrorist organizations (Fitriani & Pakpahan, 2020). Meanwhile, terrorism in the explanation of the Convention of the Organization of the Islamic Confrnece on Combating International Terrorism 1999, is an act in the form of violence or threats, which is carried out in order to terrorize others or provide threats that harm the lives of many people, self-esteem, freedom, security and rights they have, or exploit property, natural resources, private or public facilities, or control, deprive, endanger national sources or international facilities, or threaten the stability, territorial integrity, political unity and sovereignty of a state (UNODC, 2012).

So from the combined understanding of Cyberspace and Terrorism, Denning argues that Cyberterrorism is: "Unlawful attacks and threats of attacks on computers, networks, and information stored in them when carried out to intimidate or force the government or its people to pursue political or social interests." (Arifah, 2011)

Cyber terrorism attacks on anything connected to the internet, especially vital objects belonging to the government that can interfere with its functioning and can even cause greater casualties than terrorism with a conventional modus (Headquarters, 2016). The state is required to be able to control the Internet world to find out terrorist acts because Cyber terrorism has become a world issue(Brenner, 2007).

The more rapidly a new technology develops, the more sophisticated the media and modus opernadi used by terrorists so that the greater the chance that criminal acts of terrorism can occur (Situmeang, 2020).

According to the United Nations Office on Drugs and Crime (UNODC) in its research summarized in a diagram below, as many as 7% of UNODC member countries agree that Cyber terrorism is one of the crimes that is considered to have a considerable damage if it hits a country (Smith, 2015). According to Enver Bucaj in his research, it was concluded that the high number of Cyber terrorism until now has not been balanced by the existence of special regulations that can be used to overcome cyber terrorism crimes globally (Noor, 2005). In fact, establishing a global legal basis to fight Cyber terrorism is very important. Various forms of criminal acts that are used as the modus operandi used by terrorists in committing cyber terrorism crimes are also one of the reasons why there is a need for special regulations for the enforcement of Cyber terrorism crimes (Ismail, 2009)

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10183568

One of the methods or modus operandi used by terrorists in committing cyber terrorism crimes is the spread of propaganda, national law and international law have not regulated the crime of spreading propaganda, even though the effect of the propaganda crime is quite large and affects the life of a country (Arief, 2000).

If regulations regarding one form of Cyber terrorism are not yet available, it will make it difficult for a country to enforce its crimes (Juned et al., 2022). The importance of regulation regarding Cyber terrorism is also not only due to the absence of specific regulations governing these crimes, but also because of the position of cyber terrorism which is a form of transnational organized crime (MR, 2012).

Aspecial characteristic that belongs to terrorism but is not possessed by other conventional crimes, the crime is carried out in a structured and widespread and organized manner so that it becomes a very serious threat to society, nation and state. Therefore Cyber terrorism belongs to the category of "Transnational Organized Crime" (Subagyo, 2018).

The wide scope of this Cyber terrorism case makes the national law will not be enough to solve cyber terrorism cases (Rollins et al., 2010). In addition, the inclusion of cyber terrorism into the category of transnational organized crime makes the arrangements governing this crime must be many (McQuade, 2009).

B. DISCUSSION

1. Cyber-Terrorism as a Form of Crime in the Field of Cybercrime

Terrorists utilize information technology to influence the wider community and get attention to their goals. They use information technologies, such as telecommunications, computers and the internet, as tools to regulate conventional attacks (Gultom & Elisatris, 2005). In cyber terrorism, using information technology will radically disrupt internet-connected services. For example, cyber terrorists can hack into residential networks to obtain critical financial information or disable network emergency systems (Centre, 2018). Cyber terrorism is the use of the internet for terrorist activities such as the massive interference of computer networks, especially computers connected to the internet, by means of computer viruses (Harjoko, 2010).

Cyber terrorism is a form of crime in Cybercrime. Istilah "Cybercrime" has the same meaning or synonyms with several words, including: technological crime, high technology crime, high tech crime, economic crime, internet crime, digital crime, or electronic crime, these synonyms are some other words used to describe crimes committed with computers or other information technology by people (Panjaitan et al, 2005).

But actually Cybercrime is a broad term that encompasses the whole way that computers and other types of portable electronic devices such as mobile phones and PDAs that have the capacity to connect with the Internet, are used to break the law and cause harm.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10183568

The technical definition of Cybercrime is where a computer or other electronic device is used to facilitate illegal behavior through information systems such as organizational networks or the internet (Hafidz, 2014).

Barry Collin, a researcher at the Institute for Security and Intelligence in California, coined the term "Cyber terrorism" in the 1980s. This concept consists of two elements, namely: the element of cyberspace and terrorism. Cyberspace can be considered as a place where computer programs function and a place where data moves (Astuti, 2015). In 1990 the National Academy of Science began a report on computer security with the phrase "We are at risk. Increasingly, America is dependent on computers. Tomorrow, terrorists may be able to do more damage by using keyboards than bombs". It was at this time that the term "pearl harbor elektronic" was coined, which linked the threat of computer attacks to American history (Putri & Budiono, 2019).

From a psychological perspective, these two greatest fears of modern times are combined in the term "Cyber terrorism". Like Cybercrime, Cyber terrorism also has many different definitions, including: James Lewis, defines Cyber terrorism as the use of cyber computer networks and internet tools to break down critical national infrastructure (such as energy, public transport, government activities, etc.), or it can be to intimidate or coerce the government of a country or its citizens (Josianto, 2014).

The Cambridge Center for Risk Studies defines Cyber-terrorism as follows: "Cyber terrorism is an act of politically motivated violence involving physical damage or personal injury caused by remote digital interference with technological systems." (Ramli, 2004)

In addition, Dorothy Denning, a professor of computer science, has put forward a very clear definition in many articles and in her testimony on the subject before The House Armed Services Committee in May 2000, that:

"Cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful and threatening attacks on computers, networks, and information stored on them when carried out to intimidate or coerce the government or its people to enhance political or social purposes."

Furthermore, to qualify as Cyber terrorism, an attack must generate violence against people or property, or at least cause enough harm and generate fear. An attack that causes death or bodily injury, an explosion or severe economic loss would be an example. A serious attack on critical infrastructure can be an act of "Cyber terrorism" depending on its impact (Ersya, 2017).

The Federal Bereau of Investigation (FBI) describes Cyber terrorism as the development of terrorist capabilities provided by new technology and network organizations, which allow terrorists to conduct their operations with little or no physical risk to themselves" focused on "the physical destruction of information hardware and software, or physical damage to personnel or equipment that uses information technology as a medium (Danuri & Suharnawi, 2017).

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10183568

This cyber terrorism can be considered as: "The planned use of disruptive activities, or threats with targeted computers and/or networks, intended to cause harm or social, ideological, religious, political or similar purposes, or to intimidate anyone in further progress. of that purpose." Cybercrime includes unauthorized network breaches and theft of intellectual property and other data; this can be financially motivated, and the response is usually the jurisdiction of law enforcement agencies (Widodo, 2013).

Thus, a middle line can be drawn that Cyber terrorism is an act that involves both active and passive activities. Active means using computers to infiltrate critical infrastructure in a country, such as electricity, emergency services, telecommunications, water supply, economy, military, and financial institutions of a country that can be fatal. The passive side shows that Cyber terrorism can also recruit, seek support, and carry out propaganda with the aim of spreading fear to the global community in cyberspace. (Widiyanto, 2017)

According to DCSINT Handbook No.1.02, Cyber operations and Cyber terrorism, which is used to train U.S. agencies, internet operations consist of internet terrorism and internet support, expressed through planning, recruitment and propaganda. With this kind of activity, computer networks can be used as weapons, as intermediate targets or as activities that precede or follow physical attacks. Themost important goal of Cyber terrorism is the loss of integrity of the target itself, reducing the likelihood of its actions, lack of trust, security, and safety, and ultimately physical destruction (Maskun et al., 2013).

2. Criminal Law Policy in Tackling Cyber Terrorism

Cyber terrorism is part of Cybercrime and criminal terrorism. And given the borderless nature of Cyber terrorism, Cyber terrorism can be categorized as a transnational crime. Based on the perspective of transnational crime, there are two or more countries that have jurisdictional authority to enforce cyber terrorism, so that the legal instruments used as a source of enforcement can be guilty of a country's national law and the source of international criminal law (Wahyudi, 2013).

The most common motivations identified in Cyber terrorism are extortion, the desire to be destroyed, various types of exploitation and revenge. And the most common acts committed or threatened by terrorists are physical destruction, destruction of important data and information, attacks on critical computer systems, illegal invasions into computer systems of the public interest and denial of access to important systems, services and data (Kartiko, 2014).

Indonesia has two legal instruments that can be used as a source of law for enforcing cyber terrorism, namely Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, and Law Number 5 of 2018 concerning Amendments to the Law- Law Number 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism. And according to international criminal law, there are several international conventions that can be used as legal instruments for regulating cyber terrorism (Arief, 2007).

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10183568

Law No. 11 of 2008 is a law that regulates technology-based crimes (cyber crime), while cyber terrorism is part / type of cyber crime. The criminal provisions in the ITE Law are contained in Chapter XI Article 45 to Article 52.

The following is the formulation of several articles in Chapter XI regarding criminal provisions. Based on the provisions of the articles in Chapter XI regarding criminal provisions in the ITE Law, several prohibited acts (elements of criminal acts) that are closely related to cyber terrorism crimes can be identified in each article, as follows; Article 30 Relates to the crime of Cyber terrorism in the form of unauthorized access to computer systems and services (Suharyo, 2010).

Article 31 relates to the act of hacking. This law is related to cyber terrorism crimes in the form of cyber sabotage and extortion. Article 33 concerns the crime of Cyber terrorism in the form of unauthorized access to computer systems and services. Therefore, it appears that the perspective of the Electronic Information and Transactions Act is to emphasize the aspects of the use/ security of Electronic Information Systems or Electronic Documents (Bahri et al., 2019), and the misuse in the field of technology and electronic transactions carried out by cyber terrorism actors (Napitupulu, 2017).

The regulation of Cyberterrorism can also be seen in the Criminal Code Bill as follows:

a) In book I, the general provisions of the Criminal Code made provisions regarding several understandings made about several understandings related to computer networks.

b) In book II (Criminal Acts): Changes are made to the formulation of delik or add new details related to technological advances, in the hope that it can also capture cases of cyberterrorism,

c) Chapter V of the Act of Crimes Against Public Order, including: 1) Intercepting speech in a closed room with aids or technical devices (art. 263/300); 2) Installing technical aids for the purpose of hearing / recording speech (art. 264/301); 3) Recording (owning/broadcasting) images with technical aids in a public room (art. 266/303);

d) Chapter VII (Criminal Acts Endangering the Public Interest of People, Goods, and the Environment): 1) accessing computers without rights (art. 368,371, 372, 373 of the 2004 Concept); 2) damaging/making unusable buildings or facilities/ infrastructure of public services (e.g. communication buildings/ communication via satellite/long-distance communication) article. 630/ 2004;

Given the global nature of cyberterrorism crimes, investigative agencies must cooperate and have international relations so that the investigation process can be carried out quickly, effectively and appropriately (Arif, 2006). This is important, because the solution to cyberterrorism can only be done at the international level and not resting solely on individual countries.

Cyberterrorism is not only a national problem but an international problem. This crime is gaining considerable attention. The 8th UN Congress in Havana, the Xth Congress in

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10183568

Vienna, the 2005 XI congress in Bangkok, talked about The Prevention of Crime and the Treatment of Offender. In the UN X Congress, it was stated that member states should seek harmonization of relevant provisions on criminalization, evidence, and procedure, and EU countries that have seriously integrated regulations related to the use of information technology into existing legal instruments its national (Jannah & M. Naufal, 2012).

The international conventions are the United Nations Convention against Transnational Organized Crime Palermo, Italy in 2000; Budapest's Convention on Cybercrime in 2001; and the International Convention for the Suppression Of Terrorist Bombing New York, United States in 1998 (Crimes, 2007). The elements of criminal acts regulated in the three conventions have been proven to be in accordance with the elements of cyber terrorism, so that the international conventions can become legal instruments for regulating cyber terrorism (Wibawa, 2017)

In addition to the efforts made by the United Nations to rally international cooperation to tackle cyberterrorism and find solutions to problems of reporting, investigating, finding, and improving the way of proof (Collin, n.d.). Several organizations have emerged that take the initiative to create global institutions to fight cybercrime, especially cyberterrorism. The institutions such as, International Services on Discovery and Recovery of Electronic and Internet Evidences, International Organisation on Computer Evidence (IOCE), GECDInitiatives, Efforts of G-7 and G-8 Groups (Alfian, 2017).

C. CONCLUSION

Cyberterrorism is a form of terror transformation carried out by terrorists by making the internet network a tool or target of attacks. This type of crime metamorphoses into a crime of a transnational nature. The perpetrators can come from any region of the country which has legal repercussions on identity which has implications for determining the jurisdiction of the court. With this fairly advanced pattern, global or interstate cooperation is needed. One solution is that every country must synchronize the laws and regulations that specifically regulate cyberterrorism.

Indonesia has two legal instruments that can be used as a source of law for enforcing cyber terrorism, namely Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, and Law Number 5 of 2018 concerning Amendments to the Law- Law Number 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism. And according to international criminal law, there are several international conventions that can be used as legal instruments for regulating cyber terrorism.

The international conventions are the United Nations Convention against Transnational Organized Crime Palermo, Italy in 2000; Budapest's Convention on Cybercrime in 2001; and the International Convention for the Suppression of Terrorist Bombing New York, United States in 1998. In addition to the efforts made by the United Nations to rally international cooperation to tackle cyberterrorism and find solutions to problems of reporting, investigating, finding, and improving the way of proof.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10183568

Several organizations have emerged that take the initiative to create global institutions to fight cybercrime, especially cyberterrorism. These institutions include, International Services on Discovery and Recovery of Electronic and Internet Evidences, International Organisation on Computer Evidence (IOCE), GECD Initiatives, Efforts of G-7 and G-8 Groups.

Bibliography

1) Alfian, Muh. (2017). Penguatan Hukum Cyber Crime Di Indonesia Dalam Perspektif Peraturan Perundang-Undangan. Jurnal Kosmik Hukum, 17(2).

2) Anggraeni, R. D., & Rizal, A. H. (2019). Pelaksanaan Perjanjian Jual Beli Melalui Internet (E-Commerce) Ditinjau Dari Aspek Hukum Perdataan. SALAM: Jurnal Sosial Dan Budaya Syar-i, 6(3), 223–238.

3) Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 5(1).

4) Arief, B. N. (2000). Tindak Pidana Mayantara, Perkembangan Kajian CyberCrime di Indonesia. PT. Raja Grafindo Persada.

5) Arief, B. N. (2007). Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia. Rajawali Pers.

6) Arif, B. N. (2006). Tindak Pidana Mayantara dan Perkembangan kajian Cyber Crime di Indonesia. Rajawali Pers.

7) Arifah, D. A. (2011). Kasus Cybercrime Di Indonesia Indonesia's Cybercrime Case. Jurnal Bisnis Dan Ekonomi (JBE), 15(3).

8) Astuti, S. A. (2015). Law Enforcement of Cyber terrorism ini Indonesia. Jurnal Rechtsidee, 2(2).

9) Bahri, S., Yahanan, A., & Trisaka, A. (2019). Kewenangan Notaris Dalam Mensertifikasi Transaksi Elektronik Dalam Rangka Cyber Notary. Repertorium: Jurnal Ilmiah Hukum Kenotariatan, 142–157.

10) Bobic, M. (2014). Transnational organised crime and terrorism: Nexus needing a human security framework. Global Crime, 15(3–4), 241–258.

11) Brenner, W. (2007). Cybercrime: Re-Thinking Crime Control Strategies, dalam Yvonne Jewkes. Willan Publishing.

12) Centre, T. (2018). Handbook of Good Practices to Support Victims' Associations in Africa and the Middle Eas. UNCounter-.

13) Collin, B. (n.d.). Cyber terrorism is real- is it? Introduction in the 1980's Barry Collin. http://www.intelligence-andinvestigations.com/media/uploads/62_Cyberterrorism - Nicholas Bradley.pdf

14) Crimes, L. on C. (2007). Alongwith IT Act and Relevant Rules, Book Enclave.

15) Danuri, M., & Suharnawi. (2017). Trend Cyber Crime Dan Teknologi Informasi Di Indonesia. Jurnal INFOKAM, XIII (2).

16) Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. Journal of Moral and Civic Education, 1(1).

17) Fitriani, Y., & Pakpahan, R. (2020). Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace. Analisa Penyalahgunaan Media Sosial Untuk Penyebaran Cybercrime Di Dunia Maya Atau Cyberspace, 20(1).

ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10183568

18) Gani, H. A., & Gani, A. W. (2019). Penyelesaian Kasus Kejahatan Internet (Cybercrime) dalam Perspektif UU ITE No.11 Tahun 2008 dan UU No.19 Tahun 2016 (p. 121). Prosiding Seminar Nasional LP2M UNM.

19) Gultom, D. M. A. M., & Elisatris. (2005). Cyber Law (Aspek Hukum Teknologi Informasi). Rafika Aditama.

20) Hafidz, J. (2014). Kajian Yuridis Dalam Antisipasi Kejahatan Cyber. Jurnal Pembaharuan Hukum, 1(1).

21) Harjoko, A. T. P. (2010). Cyber Crime dalam Perspektif Hukum Pidana. Universitas Muhammadiyah Surakarta.

22) Headquarters, U. N. (2016). Report of the UN Conference on Human Rights of Victims of Terrorism.

23) Ismail, D. E. (2009). Cyber Crime di Indonesia. Jurnal Inovasi, 6(03).

24) Ismoyo, D. W. (2014). Kendala Penyidik Dalam Mengungkap Tindak Pidana Penipuan Online Melalui Media Elektronik Internet (Studi di Polres Malang Kota). Jurnal Hukum Universitas Brawijaya Malang, 2(1).

25) ITU. (2009). Understanding Cybercrime Guide, ICT Appliccation dan Cybersecurity Division.

26) Jannah, H. S., & M. Naufal. (2012). Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif Dan Hukum Islam. Jurnal Al-Mawarid, XII (1).

27) Josianto, A. (2014). Tindak Pidana Cyber terrorism Dalam Transaksi Elektronik. Jurnal Lex Administratum, 3(3).

28) Juned, M., Samhudi, G. R., Akhli, R. A., & Teja, M. (2022). The Social Impact of Expanding the Indonesian Military Mandate on Counter-terrorism. Aspirasi: Jurnal Masalah-Masalah Sosial, 13(1), 105–115. https://doi.org/10.46807/aspirasi.v13i1.2987

29) Kartiko, G. (2014). Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional. Politeteknik Negeri Malang.

30) Maqableh, M., Obeidat, A., & Obeidat, Z. (2021). Exploring the determinants of internet continuance intention and the negative impact of internet addiction on students' academic performance. International Journal of Data and Network Science, 5(3), 183–196. https://doi.org/10.5267/j.ijdns.2021.6.014

31) Martin, J. M., & Romano, A. T. (1992). Multinational Crime-Terrorism, Espionage, Drug & Arms Trafficking. SAGE Publications Inc.

32) Maskun, M., Manuputty, A., Noor, S. M., & Sumardi, J. (2013). Kedudukan Hukum Cyber Crime Dalam Perkembangan Hukum Internasional Kontemporer. Masalah-Masalah Hukum, 42(4), 511–519.

33) McQuade, S. C. (2009). Encyclopedia of Cybercrime. USA: Greenwood Pers the Concise Oxford Dictionary of Current English (8th edition). 1990. Clarendon Press.

34) MR, A. (2012). Yuridiksi dan Transfer of Procedding Dalam Kasus Cybercrime. Tesis, Program Studi Magister Hukum Universitas Indonesia.

35) Nadu, T. (2017). Internet marketing to improve brand awareness. 3(3), 89–91.

36) Napitupulu, D. (2017). Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional. Deviance Jurnal Kriminologi, 1(1), 100–113.

37) Noor, A. F. (2005). Tinjauan Yuridis terhadap Cybercrime di Indonesia.

38) Panjaitan, H. I., & Dkk. (2005). Membangun Cyber Law Indonesia Yang Demokratis. IMLPC.

39) Putri, C. C., & Budiono, A. R. (2019). Konseptualisasi Dan Peluang Cyber Notary Dalam Hukum. Jurnal Ilmiah Pendidikan Pancasila Dan Kewarganegaraan, 4(1), 29–36.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10183568

40) Ramli, A. M. (2004). Cyber Law dan HAKI dalam Sistem Hukum Indonesia. Refika Aditama.

41) Rapporteur, T. S. (2010). Protection Human Rights and Fundamental Freedoms while Countering Terrorism, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism: Ten Areas of Best Practices in Countering Te. http://www.ohchr.org/EN/Issues/Terrorism/Pages/Annual.aspx.

42) Rollins, J., Wyler, L. S., & Rosen, S. (2010). International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress. Congressional Research Service.

43) Sadino, S., & Dewi, L. K. (2021). Internet Crime Dalam Perdagangan Elektronik. Jurnal Magister Ilmu Hukum, 1(2), 9–17.

44) Sari, D. C., Effendy, F., Sudarso, A., Abdillah, L. A., Fadhillah, Y., Fajrillah, F., Setiawan, Y. B., Simarmata, J., Watrianthos, R., & Jamaludin, J. (2020). Perdagangan Elektronik: Berjualan di Internet. Yayasan Kita Menulis.

45) Sitompul, J. (2012). Cyberspace, cybercrime, cyberlaw, Tinjauan Aspek Hukum Pidana. PT. Tatanusa.

46) Situmeang, S. M. T. (2020). Cyber law. CV Cakra.

47) Smith, S. A. (2015). Terrorism in Southeast Asia: The Case of the Abu Sayyaf Group and Jemaah Islamiyah. International Institute for Counter-Terrorism, 33(1).

48) Subagyo, A. (2018). Sinergi Dalam Menghadapi Ancaman Cyber Warfare. Jurnal Pertahanan & Bela Negara, 5(1), 89–108.

49) Suharyo. (2010). Laporan Penelitian Penerapan Bantuan Timbal Balik Dalam Masalah Pidana Terhadap Kasus-kasus Cybercrime. BPHN Departemen Hukum dan HAM RI.

50) Theohary, C. A., & Rollins, J. W. (2015). Cyberwarfare and Cyber terrorism: In Brief. Congressional Reseach Service.

51) UNODC. (2012). The Criminal Justice Response to Support Victims of Acts of Terrorism. Vienna.

52) Vilic, V. (2017). Cyber terrorism on The Internet and Social Networking: A Threat to Global Security. International Scientific Confrence on Information Technology and Cata Related Research Serbia. Singidunum University.

53) Wahyudi, D. (2013). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia. Jurnal Ilmu Hukum Universitas Jambi.

54) Wibawa, I. (2017). Cyber Money Laundering (Salah satu bentuk White Collar Crime abad 21). YUDISIA, 8(2), 241.

55) Widiyanto, B. (2017). Dampak Serangan Virtual ISIS Cyber Calipathe Terhadap Amerika Serikat. Jurnal International & Diplomacy. Universitas Paramadina Jakarta, 2(2).

56) Widodo. (2013). Hukum Pidana di Bidang Teknologi Informasi, Cybercrime Law: Telaah Teoritik dan Bedah Kasus. Aswaja Pressindo.

57) Zakaria. (2012). Analisis Hubungan Hukum Dan Akses Dalam Transaksi Melalui Media Internet. Jurnal Hukum, 2(2).