ISSN 2614-0047

Cyber terrorism in Indonesia

Katya Lindi Chandrika [1,*], Risky Perdana Adiperkasa [2], Yana Ningtyas [3]

Department of Electrical Engineering, State University of Malang, Malang, Indonesia
[1] katyachandrika@gmail.com*; [2] riskyperdana999@gmail.com; [3] yananingtyas@gmail.com
* corresponding author

ARTICLE INFO

Article history
Received September 4, 2018
Revised September 30, 2018
Accepted October 11, 2018

Keywords
Cybercrime
Cyber terrorism
Terrorism

ABSTRACT

Cyber terrorism is one of cybercrime. Cyber terrorism is an activity using computer technology and information to create an atmosphere of terror and fear on a large scale through good threats to the government and citizens with brings politics, religion or ideology objectives which can lead paralysis of important infrastructure. There are several reasons why the internet is considered as the right choice to do Cyber terrorism. Many methods are used to do Cyber terrorism. In Indonesia, people's understanding about Cyber terrorism is very low. This creates ignorance in tackling Cyber terrorism crime in the future when people become victims of Cyber terrorism. The low knowledge about Cyber terrorism requires the government to make education about Cyber terrorism. The education provided will help people find solutions in the against Cyber terrorism. In avoiding Cyber terrorism crime the government is expected to cooperate with other developed countries that have a high level of security.

1. Introduction

Humans in this modern era cannot separate from many activities. Human activities sometimes are largely beyond human control and capability. Human inability to handle every activity and problem that exist, causing humans need something can help the disability. One way human in resolve these problems by utilizing technology. Today's technology is growing very rapidly and will progress as science progresses.

One form of technological advancement is the existence of cyber technology. Cyber technology that connected with many internet networks has made new phenomenon in every stage of human interaction in cyber space. Cyber technology is the use of the internet as media for communication and interaction without limit. Cyber technology then make negative impacts such as emergence crime via cyber media usually known as cybercrime.

The irresponsible use of cyber can result in the occurrence of violations or crimes which may result in the occurrence of a particular threat to the state. The type and violation of cybercrime very diverse as a result of improper use. Wiretapping, theft and misuse of information or data in an electronic form or electronically transferred, illegal fund rising, destruction of websites and system through viruses, Trojan horse, signal grounding and the like are forms of cybercrime. These emerging crimes need to be wary of their development.

There are several types of cybercrime, one of them is a crime that raises terror and anxiety in the people cause harm to the state. The crime is Cyber terrorism. However, Cyber terrorism is still unknown to the layman. This is because ordinary people do not form of crime so they assume normal and do not want to know about Cyber terrorism. Ignorance about Cyber terrorism cause the public not to know how to prevent and overcome Cyber terrorism.

2. Cyber Terorrism

Cyber terrorism is a combination of two words which are cyber and terrorism. Cyber means cyberspace, and terrorism is an act of violence and intimidation in the pursuit of political aims. What people first thought of Cyber terrorism, it comes to war, radical organization and other rebellious activity. In reality, the definition of Cyber terrorism not as simple as that.

The definition of Cyber terrorism always been a debate since the 1990s. The debate of definition occurred because it is not easy to explain how terrible the damage caused by a single computer attack. The term Cyber terrorism has become controversial. Sometimes the term of Cyber terrorism is used in different contexts.

The term Cyber terrorism was first introduced by Barry Collin in 1980 as a transition of terrorism from the physical world to the virtual world [1]. The Center for Strategic and International Studies (CSIES) defines this term as the use computer networks to paralyze the state infrastructure such as transportation, government, energy and other devices [2][3] [2][3]. Then William L. Tafoya, a retired FBI special agent describes Cyber terrorism as intimidation through the use of technology with political purpose, religion or ideology can result in paralysis of important infrastructure and important infrastructure information data [4]. Uma and Padmavathi define the term Cyber terrorism as the use cyberspace to create large scale disruption and destruction of life and property [5].

Over time, in all cycles the definition transformed into the use of information technology to run an activity of terrorism [6]. Surely there is not precise definition to describe the term Cyber terrorism. However from the definitions that presented, it can be conclude that Cyber terrorism is the activity of the use computer and information technology to create an atmosphere of error and fear of large scale through threats for government and citizens with brings politics, religion or ideological objectives which can lead paralysis of important infrastructure.

The term of Cyber terrorism was first introduce in 1980. This term then became more pronounced after attack on September 11, 2001 in World Trade Center. The attack led to many areas of government to review the standards and procedures of their security system. It also increase awareness that terrorists can use other way to reach their goals including Cyber terrorism [7].

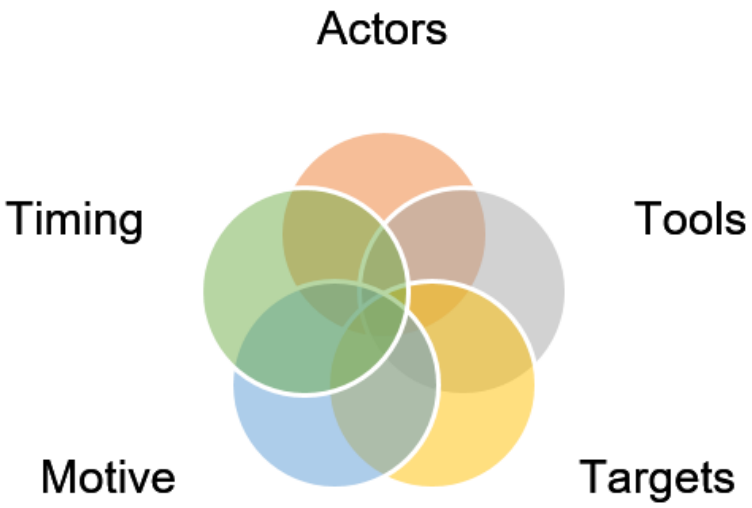

Fig. 1. Anatomy of cyber terrorism.

Bradley K. Ashley in his paper titled "Anatomy Of Cyber terrorism: Is America Vulnerable?" Mapping and anatomical model of Cyber terrorism. There are 5 factors of cyber terrorism which can be seen in Figure 1. The first factor is an actor, Colarik confirmed in a statement that *there is no Cyber terrorism without terrorism, period*. The statement confirmed that Cyber terrorism actor are terrorists. they launched their terror activity using cyber facilities. The second one is tools, the occurrence of Cyber terrorism is certainly on the base that an important infrastructure of country works and depends on the utilization computer network. The next factor is a target, currently countries in the world are highly dependent on information systems. The information system are used as a basic needs for country to reserve public interest. So Cyber terrorism always targets its target on infrastructure that has critical information. Infrastructure that quite important and usually as targeted by Cyber terrorism

attacks are: (a) Telecommunications, (b) Health, (c) Defense, (d) Government, (e) Banks, (f) Energy, and others. The fourth factor is a motive, in general there are motives why the internet is often a tool or target where the occurrence of crime. According to Phillip W. Brunst the factors become the motivation of crimes commited on the internet are: (a) Location, (b) Speed, (c) Anonymity, (d) wide coverage, and (e) Cost-Benefit Ratio. And the last factor is a timing, attacks can be done anytime. The time of attack will be grealty determined by the right momentum so that fear can spread widely among the people. In other words, the timing of attack will be correlated with the objectives, capabilities and vulnerability factors of the security system of network is used as a tool or target attack.

Cyberspace is a technology that is often used become tool or target where occurrence of crime. Cyber-attacks offer terrorist abilities to launch their actions with the greater effect, create greater damage to a country and pose a direct threat then they do physically. The traditional terrorist activity such as bombing will cause trauma effects that are only limited to that location alone [3][4]. In addition, there are several reasons why cyberspace is chose to launch acts of terrorism summarized in Table 1.

Table 1. The Reason Terrorist Use Cyberspace

No.	Reason	Detail
1.	Anonymity	Cyberspace offers anonymity, attacks can be disguised with specific programs or techniques, self-information is difficult to trace [10] The difficulty of knowing the motives of terrorists using cyberspace.
2.	Access	can attack wherever they are, whether near or far from the location. using worms and viruses to spread without any direct involvement. When the attack has been designed, the terrorist can start quickly without requiring more preparation.
3.	Communication	Used a media to discuss the attack plan. Free control of mass in large quantities [1] As an alternative to train members in the form of instruction or audio. For example how to make bombs, firearms and something dangerous.
4.	Resource	Using less resources, but the resulting effect is greater. As terrorists who have limited funds
5.	Propaganda and Recruitment	For propaganda action, usually an explanation of ideology, practical instruction and promotion of terrorist activities. Usually present in multimedia form. Propaganda distributed over the internet can easily spread widely. Recruitment of terrorist groups is based on lure, resentment and weakness in thinking. Recruiting many members becomes easier.

Cyber terrorist use various methods to launch their actions [11]. The following descriptions are some of the methods often used by terrorists. The first method is a hacking. Hacking is an activity braking into someone else is computer or can be said as any form of unauthorized access to computer or computer network. Hacking itself can be a form threat “cyber murders”. The next method is Trojan, is a program will pretend work as good and useful program but actually do the activities of spying and stealing data. Computer Worms, this is a kind of malware (Malicious Software) that can activated itself. When malware successfully enter in computer or network then worm can move to another computer in one network automatically. Cryptography, the encoding of data in the text form or video (encryption) and the laying of hidden sentence on an object is used by terrorist to ensure their message is confidential [12]

Until now, there are several cases of Cyber terrorism that occur in the world. In 2008, there was a plane crash at Madrid-Bajaras airport where one of Spanair’s central computers was infected by Trojans. The plane will send a signal when there are some technical problem and the central computer should generate an alarm. Until the plane dropped because the alarm was not reached and cause 154 deaths. It is considered airlines failure to secure central computer from the dangerous code of external infection. This event makes people assume that the vital system is not always protected and affects the public's trust in the capacity and readiness of the authorities to deal with risks, vulnerabilities and crises, something that may have long-term political implications [13].

Another case occurred in 2012, the New York Times reported cyber-attacks by the United States and Israel against Iran. This cyber-attack uses computer virus Stuxnet to cripple Iran's nuclear program. The attack using Stuxnet Malware is not the first time experienced by Iran. Stuxnet Malware

Attacks have occurred in 2009 during the installation of nuclear enrichment. Stuxnet malware is capable on sabotaging the motor system of the nuclear drive. The Iranian government also often gets cyber-attacks carried out by a number of foreign countries. This attack is considered a cyber-security threat and cyber terrorism against the state.

In 2014 ISIS spread propaganda on twitter and always provide the latest information. This information is like bombing, suicide missions, and assassinations, checkpoints in the cities they control, photographs of arrests, transport and massacres of detainees. The information they shared eventually spread quickly on the internet because it was disseminated by pro-ISIS. Although not sure whether the account is purely made by ISIS or not, it makes people in the world anxious.

ISIS opened a Google Plus account for several months. The opening of this account is not realized by Google. This account is used to disseminate ISIS information for pro-ISIS. Other cases of Cyber terrorism occur in Estonia. In the case of Estonia, Cyber terrorism occurs through the widespread use of "zombie" computer botnets. Hackers hack computers-including home PCs-in Egypt, Russia and the United States and use them in DDoS strategies. Government and bank sites that typically receive 1,000 visits per day fall after receiving a 2,000 increase per second. [3]

Especially in Indonesia, Bali bombing is a case of cyber terrorism that became history in Indonesia. Imam Samudra who is one of the figures who caused the Bali bombing tragedy stated that the internet facilitates him in committing the crime. Commissioner General Makbul Padmanagara told the IDEC conference that Indonesia could uncover cases of cyber terrorism for the first time the case was linked to the Bali bombing case.

In 2006, Police arrested two people suspected of Cyber terrorism by buying a domain www.anshar.net for propaganda radicalism [14]. in early 2016 there was a bomb explosion in Thamrin area, Jakarta. Polri stressed that the network of terrorism "Bahrun Naim" is communicating using social media. The application used is Telegram. The procedure for making bombs is also distributed and can be downloaded by followers.

In May 2017, there was a cyber-attack in several countries including Indonesia. Cyber-attacks "ransomware", a software or malicious software that attacks the computer by encrypting the victim's computer data so it cannot be accessed. Ransomeware is named WannaCry. The victim must pay some money if the data does not want to be permanently deleted. Because of wannacry, information systems of two hospitals in Indonesia cannot keep patient data and hospital payments. According to Sammy Pangerapan, Director General of Informatics Applications in Indonesia, this attack is Cyber terrorism because it threatens and cripples critical infrastructure.

From the psychological side, people become worried, anxious, intimidated and scared [15]. The internet has become a part of human life, the fear will also increase. Cyber terrorism that attacks infrastructure and vital objects causes huge losses. Cyber terrorism can disrupt economic stability and can be used to threaten political opponents.

3. Cyber terrorism According to Society in Indonesia

To find out the understanding and opinion of Indonesian society on Cyber terrorism, a survey was made with 10 questions shown in Table 2. The questionnaire was distributed online. After five days, data obtained answers from 128 respondents. From the 128 respondents, 41% did not know the term Cyber terrorism. The misconception of the definition of Cyber terrorism can also be seen in Figure 2. 34% of respondents chose that Cyber terrorism is a terrorist who breaches or alters databases in government and terrorists who commit identity theft. 34% of respondents have misinterpreted Cyber terrorism as another cybercrime action.

Although the percentages show low results, it shows a lack of public knowledge of the increasingly modern terrorism. Speaking of Cyber terrorism as a threat to Indonesia, almost all respondents, or 95% of respondents consider Cyber terrorism a threat to Indonesia. Very surprising, in other words even though there are respondents do not know about what Cyber terrorism is, respondents assume that it is a threat to Indonesia. While the government's rating in educating the public about Cyber terrorism, preventing, and overcoming Cyber terrorism. The average score given by respondents is 2,8; 3,04; and 3,05 out of 5. This shows, the Indonesian government has tried its best to handle Cyber terrorism. In the education of Cyber terrorism, the respondents gave an average of half the rating that

meant that the respondents considered that the government should improve the education of Cyber terrorism.

Table 2. Questionnaire of The Cyber terrorism Understanding for Indonesia

No.	Question	Answer
1.	Gender	Men / Women
2.	Age	Under 17
		17 until 25
		26 until 45
		Above 45
3.	What activities are being undertaken by respondent	School (Elementary, Primary, High)
		Diploma (D1/D3/D4)
		College (S1/S2/S3)
		Work
		Does not work
4.	Respondent's knowledge about computer	Average / High / Basic / Advance
5.	Does respondent know about Cyber terrorism	Yes / No
6.	Exact defenition of Cyber terrorism according to the respondent	Attacks with political motives committed on infrastructure such as airports and power stations, causing damage (2)
		Terrorists who use computer networks as a tool to spread propaganda and member recruitment (4)
		Terrorists who do burglary / database changes to the government (3)
		Terrorists who commit identity theft and create false identity documents (1)
7.	The respondent's opinion about Cyber terrorism as a threat to Indonesia	Yes / No
8.	Rating for the Indonesian government in educating the public about Cyber terrorism	Rating 1 to 5
9.	Rating for the Indonesian government in preventing people from Cyber terrorism	Rating 1 to 5
10	Rating for Indonesian government in overcoming the public about Cyber terrorism	Rating 1 to 5

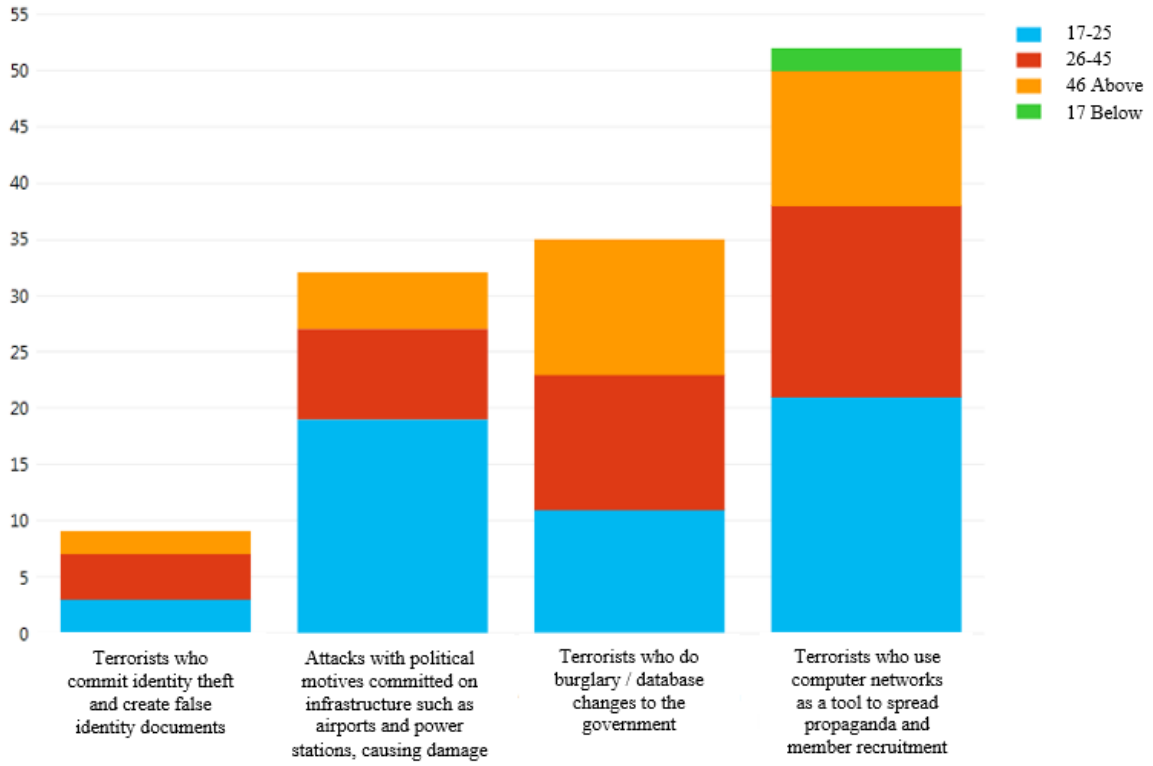

Fig. 2. Respondents' opinion about cyber terrorism terms.

4. Prevention and Solution

In Indonesia, much prevention by the Ministry of Communications and Information by blocking sites of radicalism. Although there are still many sites that have not been blocked, at least the government has reduced sites that cause propaganda and fear. Indonesia also cooperates with other countries to minimize cybercrime.

The cooperation within Indonesian police and AFP continued with the building of TNCC and Cybercrime Investigations Satellite laboratory. TNCC servers as a center for gathering analysis and exchanging information between Police and AFP, primarily in combating transnational crimes including cybercrime. The TNCC supports the full discussion of the two countries held annually in Senior Official Meeting (SOM) of the Police and AFP and represents the actual delivery contained in Memorandum of Understanding (MoU) between the Indonesian and Australian governments in tackling transnational crime. While the function of the CCIS laboratory is to monitor the activities of hackers, CCIS is also used to reveal the financing of terrorism networks that have been well accommodated. Then, with this satellite, the police can easily and quickly track and detect terrorist networks that usually communicate via email or Short Messaging Service.

Until now there has been no specific arrangement regarding Cyber terrorism in international law. In this legal vacuum situation, the ASEAN Convention on Counter Terrorism and International Convention for the Suppression of Terrorist Bombings can be used as a legal basis to criminalize Cyber terrorism perpetrators. Unfortunately, this convention did not regulate further about the elements of Cyber terrorism's criminal acts, the scope of Cyber terrorism, as well as what distinguishes it from terrorism.

In Indonesia, legislation that is still valid and effective to be linked in order to ensnare the perpetrators of criminal acts of Cyber terrorism namely the Law of the Republic of Indonesia Number 15 Year 2003 on the Crime of Terrorism and the Law of the Republic of Indonesia Number 11 Year 2008 on Information and Electronic Transactions. UU (*Undang-undang* or constitution) no. 11 Year 2008 is a law that regulates the crime-based crime technology (cybercrime), while the criminal act of Cyber terrorism is part or type of cybercrime. The criminal provisions in the Information and Electronic Transactions (IET) Act are contained in Chapter XI Articles 45 through 52. Based on the provisions of Chapter XI on the criminal provisions of the IET Act, it may be identified some prohibited acts (elements of crime) that are closely related to the criminal act of Cyber terrorism in each chapter. Article 30 Related to the crime of Cyber terrorism in the form of unauthorized access to computer system and service. Article 31 is related to hacking crime. In this law related to the crime of Cyber terrorism in the form of cyber sabotage and extortion. Article 33 concerns the crime of Cyber terrorism in the form of unauthorized access to computer system and service. Therefore, it appears that the perspective of the IET Act is emphasizing the aspects of the use or security of Electronic Information Systems or Electronic Documents, and the abuse of technology and electronic transactions conducted by Cyber terrorism actors.

Then, Indonesia also has also cooperated with other countries for Cyber terrorism prevention. On March 29, 2017, President Joko Widodo and Fancois Holland on a bilateral visit Indonesia – France agreed to establish corporation in the field of eradication of Cyber terrorism. From what has been occurred, most targets of Cyber terrorism are large organization. These organizations include government, banking, infrastructure like airport and others. There are several ways that can be used to protect country's critical infrastructure, such as: (1) Privacy, information or data from each organization must be safeguarded and not easily accessible by unauthorized users. The secret storage of communication plays an important role in security. (2) Availability, information or data that plays a leading role in the organization or in government offices should be kept secretly when it should be transparent to authorized users and should not be accessed easily by unauthorized users. This is necessary to fix some limitations for legitimate users. (3) Authentication, the identity of authorized users must be verified to access information or data before data is accessed. There are three ways available to verify a legitimate user identity, by using a password, token and biometric. With this verification method, it's easy to separate authorized users from unauthorized users. (4) Integrity, information or data should not be changed during delivery process. Information must arrive at the destination exactly as it has been sent from the source. (5) Non-repudiation, the sending and receiving party of the information or data shall ensure that both are aware of the delay in the transmission and reception of data or information.

Aside from security purpose, there are some other secondary goals needed to maintain security. They are access and availability [5]. In addition, there are also several ways that individuals can do to protect themselves and minimize the impact of Cyber terrorism. Individuals can use strong passwords, use different passwords for each website, use a more secure operating system, secure personal networks and secure data with strong encryption. Then, each individual must be must be capable in processing and sorting information. The new generation is also expected to assist in this case, by doing research that can facilitate investigation of cyber terrorism cases such as research on text classification techniques [16].

5. Conclusion

The roles of technology in assisting terrorist crimes through cyberspace are to facilitate the launch long-range attacks, cost-effective, maximum in term of disguising, easy recruitment, virus spreading, no need to bother on member training, communication media between terrorists. The impact of Cyber terrorism is destroying the country's infrastructure and making people worried, anxious, and fearful. One way to cope Cyber terrorism is by making a legislation in order to ensnare the perpetrators of criminal acts of Cyber terrorism and every individual must be capable in processing and sorting information.

The government should establish an association that helps to fight cyber terrorism, for members of the association the government can utilize human resources in Indonesia by selecting students in Indonesia, especially those who study the program or other Informatics Engineering that is able to fight Cyber terrorism. The government must block sites in the internet that contain elements of crime including terrorism, because in this era of globalization internet users not only come from adults but children also can use it. The role of parents is also very important in monitoring what their children are accessing and seeing, so crime via the Internet can be minimized.

References

[1] A. Kontselidze, "Cyberterrorism - When Technology Became a Weapon," *Eur. Sci. J.*, vol. 11, no. 10, pp. 24–29, 2015.

[2] A. Jones, "Cyber Terrorism: Fact or fiction," *Comput. Fraud Secur.*, vol. 2005, no. 5, pp. 4–7, 2005.

[3] S. Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *J. Strateg. Secur.*, vol. 4, no. 2, pp. 49–60, 2011.

[4] W. L. Tafoya, "Cyber Terror," *FBI Law Enforc.*, vol. 80, no. 1, pp. 1–7, 2011.

[5] M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and Their Classification," *Int. J. Netw. Secur.*, vol. 15, no. 5, pp. 390–396, 2013.

[6] N. Foggetti, "Cyber-Terrorism and The Right to Privacy in The Third Pillar Perspective," *Masaryk Univ. J. Law Technol.*, vol. 3, no. 3, pp. 365–376, 2014.

[7] J. J. Prichard and L. E. MacDonald, "Cyber Terrorism: A Study of the Extent of Coverage in Computer Science Textbooks," *J. Inf. Technol. Educ.*, vol. 3, pp. 279–289, 2004.

[8] M. Dogrul, A. Aslan, and E. Celik, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism," in *Cyber conflict (ICCC), 2011 3rd international conference*, 2011, pp. 1–15.

[9] M. Stohl, "Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?," *Crime, law Soc. Chang.*, vol. 46, no. 4, pp. 223–238, 2006.

[10] G. Cavaglion and E. Rashty, "Narratives of Suffering among Italian Female Partners of Cybersex and Cyber- Porn Dependents," *Sex. Addict. Compulsivity*, vol. 17, no. 4, pp. 270–284, 2010.

[11] R. Nagpal, "Cyber Terrorism in The Context of Globalization," in *II World Congress on Informatics and Law*, 2002, pp. 1–23.

[12] S. M. Furnell and M. J. Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?," *Comput. Secur.*, vol. 18, no. 1, pp. 28–34, 1999.

[13] R. Heickerö, "Cyber Terrorism: Electronic Jihad," *Strateg. Anal.*, vol. 38, no. 4, pp. 554–565, 2014.

[14] J. Y. Hui, "Studies in Conflict & Terrorism The Internet in Indonesia: Development and Impact of Radical Websites," *Routledge*, vol. 33, no. 2, pp. 171–191, 2010.

[15] L. Huddy, S. Feldman, T. Capelos, and C. Provost, "The Consequences of Terrorism: Disentangling the Effects of Personal and National Threat," *Polit. Psychol.*, vol. 23, no. 3, pp. 485–509, 2002.

[16] D. A. Simanjuntak, H. P. Ipung, and A. S. Nugroho, "Text Classification Techniques Used to Facilitate Cyber Terrorism Investigation," in *Advances in Computing, Control and Telecommunication Technologies (ACT), 2010 Second International Conference*, 2010, pp. 198–200.