[Indonesian Journal of International Law](https://scholarhub.ui.ac.id/ijil)

Volume 7
Number 3 *Human Rights Law*

Article 6

August 2021

CYBER TERRORISM PREVENTION AND ERADICATION IN INDONESIA AND ROLE AND FUNCTIONS OF MEDIA

Edmon Makarim

Cyber Terrorism Prevention and Eradication in Indonesia And Role and Functions of Media

Edmon Makarim[1]

The objective of terrorist is to create widespread fear to the society. This issue has then direct or indirect influent to the role of print and electronic media. Nowadays, the terrorist acts are carried out not only with physical violence but also by non-physical means through the medium of internet as a global communication. The main question is, whether terror groups could be protected as part of the freedom of expression. This article discusses mainly on the prevention and eradication of cyber terrorism in Indonesia and its relations to the role and function of Media.

Keywords: Cyber Terrorism, IT Law, Terrorism

I. Introduction

Recently, the public was further immersed the news about terrorism and arrest in Aceh following the news of The Bank Century case. This recent episode in a same volatile area served as a reminder the dangers of terrorism are still at large in Indonesia, although the perpetrators continue to be pursued.

Indonesia, in the post-reform era, has been on the receiving of acts of terrorism, in particular The 'Bali Bombing' as well as, and another bombings of the several foreign embassies and international hotels. Although the perpetrators have been arrested and some have received the death sentence, the resilience of nations against the misuse or misunderstanding of religion in addressing should continue to be common concern.

Related to this backdrop is that given the goal of terrorists to create widespread fear, then either directly or indirectly, the role of both print and electronic media contributes to this goal. Therefore, there is a significant possibility that the planners of terrorist acts have also calculated the effects of the media on the public, whereby such news is considered a measure of their success in showing their existence to the public. It has been stated that

---

[1] The author is currently a lecturer at Faculty of Law University of Indonesia

if developed countries began to notice this and suggested the media report proportionately the news itself, would not to be counterproductive to peace and security of society.[2]

It is interesting to note that terrorist acts not only are now carried out with physical violence or destruction, but also by non-physical means including through the medium of an open global communication (internet). Could terror groups be protected as part of freedom of expression? Certainly, this would be very interesting to be studied further as well as how far of Indonesian national legal system could prevent and cope with terrorist acts occurring through the medium of cyberspace ("cyber-terror").

II. Definition and Scope of Cyberterror

"Cyberterror" is composed of the word "cyber" and "terror", where the cyber is short for the word "cyberspace", while the word "terror" is referring to "terrorism" itself. Following legal definitions of associated terms are relevant

Terror:

Alarm; fright; dread; the state of mind induced by the apprehension of hurt from some hostile or threatening event or manifestation; fear caused by the appearance of danger. In an indictment for riot at common law, it must have been charged that the acts done were "to the terror of people."

An element of offense of aggravated kidnapping, is any act which done to fill with intense fear or to coerce by threat or force. Roger v. State, Tax.Cr. App., 687 S.W.2d 337, 341.

Terrorism :

" An act of terrorism" means an activity that involves a violent act or an act dangerous to human life that is a violation of the criminal law of the united states or of any states, or that would be a criminal violation if committed within the jurisdiction of the United States or of any states; and appears to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of the government by intimidation or coercion, or (iii) to affect the conduct of a government by assassination or kidnapping.

---

[2] Parliamentary Assembly Recommendation 1706 (2005) on Media and Terrorism.

Terroristic threats:

A person is guilty of a felony if he threatens to commit any crime of violence with the purpose to terrorize another or to cause evacuation of a building, or otherwise to cause serious public inconvenience, or in reckless disregard of the risk of causing such terror or inconvenience.

Meanwhile, the definition of "terror" related terms according to the Indonesian dictionary 2nd edition published by literature Hall is as follows:

Terror:
Attempt to create fear, terror, and cruelty by a person or group.
Terrorize:
Cruelty (arbitrarily and etc.) to create a sense of dread and fear.
Terrorist:
People who use violence to create fear, usually for political purposes.
Terrorism:
The use of violence to inspire fear in an attempt to achieve a goal (especially political purposes); practices acts of terror
Meanwhile, according to some international conventions, the definition of terrorism is as follows:

- According to the "Treaty on Cooperation among the Member State of the Commonwealth of Independent States in Combating Terrorism, signed in Minsk 4, June 1999; Terrorism is:

  "An illegal act punishable under criminal law committed for the purpose of undermining public safety, influencing decision-making by the authorities or terrorizing the population, and taking the form of:

(i) Violence or the threat of violence against natural or juridical persons;

(ii) Destroying (damaging) or threatening to destroy (damage) property and other material objects so as to endanger people's lives;

(iii) Causing substantial harm to property or the occurrence of other consequences dangerous to society;

(iv) Threatening the life of a statesman or public figure for the purpose of putting an end to his State or other public activity or in revenge for such activity;

(v) Attacking a representative of a foreign State or an internationally protected staff member of an international organization, as well as the business premises or vehicles of internationally protected persons;

(vi) Other acts classified as terrorist is under the national legislation of the parties or under universally recognized international legal instruments aimed at combating terrorism.

- According to Article 1 (3) of the OAU Convention on the Prevention and Combating of Terrorism (Algiers, 14 July 1999):

"Terrorist act" means:

a. any act which is a violation of the criminal laws of a state party and which may endanger the life, physical integrity or freedom of, or cause serious injury or death to, any person, any number or group of persons or causes or may cause damage to public or private property, natural resources, environmental or cultural heritage and is calculated or intended to:

   (i) intimidate, put in fear, force, coerce or induce any government, body, Institution, the general public or any segment thereof, to do or obtain from doing any act, or to adopt or abandon a particular stand point, or to act according to certain principles; or

   (ii) Disrupt any public service, the delivery of any essential service to the public or to create a public emergency; or

   (iii) Create general insurrection in a state. or

b. any promotion, sponsor, contribution to, command, aid, incitement, encouragement, attempt threat, conspiracy, organizing, or procurement of any person, with the intent to commit any act referred to in paragraph (A) (i) to (iii)

According to Prof. Ulrich Sieber and Phillip W. Brunst, "cyberterrorism" is the use of the Internet for the benefit of Terrorist, which includes, among other things, (a) attacks through the Internet (via hacking) that cause damage to public infrastructure, (b) disclosure of information that is against the law (dissemination of illegal content), and (c) the use of other information technology by terrorists for the purposes of terrorism.[3]

The use of the Internet for terrorist purposes, involves:

(a) attacks via the internet that cause damage not only to essential electronic communication systems and the IT infrastructure but also

[3] Prof. Dr. Ulrich Sieber and Phillip W. Brunst. Cyberterrorism – the Use of the Internet for Terrorist Purpose. (expert report), Council of Europe, December 2007, Page 11.

to other infrastructure, systems, and legal interests, including human life (public utility damage)

(b) dissemination of illegal content, including threatening terrorist attacks; inciting, advertising, and glorifying terrorism; fundraising for and financing of terrorism; recruiting for terrorism; and dissemination of racist and xenophobic material; as well as

(c) other logistical uses of IT systems by terrorist, such as internal communication, information acquisition, and target analysis.

Cyberteror can be understood as comprising two main types of behavior. The first is where the electronic system itself that connects cyberspace is the target object of the terrorism ("cyber-attacks"). The second is taking advantage of cyberspace as a medium or as a facility to support terrorism itself.

In the first category, the perpetrators of terrorism (terrorist) occurred in choose electronic systems that are vital to the public (critical infrastructure) as their target in order to make public fear. As an example of this Estonia, where the implementation of electronic systems for public service stopped because instigated of a death threat that was sent from "botnet" which has been installed underground in various servers. The attack was by Russian hackers, motivated simply because they were offended by the actions by Estonians in demolishing a Lenin statue in Estonia.

In the second category, the perpetrators of terrorism utilize the freedom of the Internet, in particular its anonymity, the low cost of communication, diverse content that can be made, access speed, distribution, expanding the scope of viewers, and the tendency of freedom of expression without any liability due to the general lack of content regulation, and that the data would be stored for long enough to enable viewing.

There are many things that Internet itself offers terrorists, among others; as a means of communication (with encryption) to design and carry out an attack, a means of funding support, a means teaching acts of terror, a means of propaganda to justify acts of terror, even the means to see the success of terrorist acts themselves. Apart from being propaganda for their existence, the interest is used it is to recruit or members terrorist group or encourage terrorism.

Considering that cyberterror has similar characteristics to cybercrime in general, cyberterror is effectively sub-set of cyberspace crimes (cybercrime). The difference can only be seen in the character of the motivation from perpetrators, which seems more driven by political motivation, ideological, religions, hatred, victims of oppression or even because of the anti-social indication of the offender.

III. Laws and Regulations Related With Terrorism Prevention and Control

After the 2002 Bali bombing incident which killed 202, the government enacted Law No.15 of 2003 on Stipulation of Government Regulation in Lieu of Law Number 1 Year 2002 Concerning the Eradication of Criminal Acts of Terrorism, (hereinafter simply called "Law of Terrorism").

In Republic of Indonesia Presidential Decree No.7 of 2005 Concerning the Medium Term Development Plan for 2004 -2009 ("Perpres RPJM") it is stated that there were acts of terrorism in Indonesia during the preceding 3 years, including the Bali bombing case in 2002 .

The extent and the target of terrorism in Indonesia extends to domestic and international interests. Even Indonesian interests abroad have become targets of terrorism as illustrated by the Indonesian Embassy bombings in France in 2004. This shows that if terrorism is not successfully and effectively addressed it will increase in intensity and frequency. The more advanced knowledge of the perpetrator(s) and the more modern technology used, the more difficult is it to detect potential ideas at an early stage and the perpetrator(s). In a presidential decree (RPJM), the government has given attention to prevention and control of terrorism.

As stated in Article 1 (1) in the Law of Terrorism, the criminal act of terrorism must satisfy to the elements of such crime contained in the terms acts of "violence" or "threats" of violence intended to creates fear or creates tremendous widespread fear, both to the public and to government.

In Paragraph (4) and (5) Article 1 are defined 'violence' and 'threat of violence'. "Violence" means any act of abuse of physical force with or without the use of facilities and which unlawfully causes harm to the body, life, and freedom of people, including making people unconscious or helpless. The definition of "threats of violence" means any act done intentionally to situation that causes fear of people or society at large.

Article 6 and Article 7 of the Law of Terrorism are the main criminal provision. Article 6 states that every person who intentionally uses violence or threats of violence led to an atmosphere of terror or widespread fear or that causes mass casualties, by seizing independence, or loss of life and property of others, or causes damage or destruction of vital objects of strategic or environmental or public facilities or international facilities, shall be punished with the death sentence or life imprisonment or imprisonment between brief 4 and of 20 (twenty) years.

Meanwhile, Article 7 states that every person who intentionally uses violence or threats of violence to create an atmosphere of terror or widespread fear or that are causing mass casualties by seizing independence or loss of life or property of others, or to cause damage or destruction of vital objects of strategic, or environmental, or public facilities, or international facilities, shall be punished with imprisonment for life.

In addition, the Law of Terrorism not only expressly imposes criminal sanctions the perpetrators but also all those who participated or provides assistance to such a criminal act similar to the perpetrator, as stipulated in Article 13[4], Article 14[5], Article 15[6] and Article 16[7] of the Law of Terrorism.

Electronic evidence is covered in Article 27, where it is stated that:

The evidence of criminal acts of terrorism shall comprise of:

a. those matters referred to an evidence in Indonesia General Criminal Procedures (Kitab Undang-Undang hukum Acara Pidana/KUHAP);

b. other evidence in the form oral information, sent, received, or stored

[4] Article 13: Any person who intentionally aids or ease of crimes of terrorism, with: (a). giving or lending money or goods or other assets to the perpetrators of criminal acts of terrorism; (b). hiding the crimes of terrorism; or (c) hiding information about criminal acts of terrorism; shall be punished with imprisonment of a minimum of 3 (three) years and maximum15 (fifteen) years.

[5] Article 14: Any person who plans and / or proves others to do the criminal act of terrorism referred to in Article 6, Article 7, Article 8, Article 9, Article 10, Article 11 or Article 12 shall be sentenced to capital punishment or life imprisonment

[6] Article 15: Everyone who plots, trial, or gives assistance to a criminal act of terrorism referred to in Article 6, Article 7, Article 8, Article 9, Article 10, Article 11 or Article 12 shall be punished the same penalty as the erpetrators of those criminal acts.

[7] Article 16: Any person outside the territory of the Republic of Indonesia that provides assistance, convenience, facilities, or information for a criminal act of terrorism, shall be punished with the same penalty as those perpetrators of criminal acts referred to Article 6, . Article. 7, Article. 8, Article. 9, Article. 10, Article. 11, Article. 12.

electronically by means of optical or similar means of electronic media to that; and

c. data, recording, or information that can be seen, read, and / or heard, which may be issued with or without the aid of a machine, whether written on paper, any physical object other than paper, or electronically recorded, including but not limited to:
    1) writing, sound, or images;
    2) maps, plans, photographs, or the like;
    3) Letters, signs, numbers, symbols, or perforations which have meaning or can be understood by those who can read or understand them.

Notably the Law of Terrorism does not restrict the validity of evidence to only in the conventional physical evidence, but expands it to encompass electronic systems. The Law of Terrorism does not specifically regulate Internet use for the purposes of terrorism, however this does not mean the Law of Terrorism cannot be applied to cyberspace activities.

In this regard, in relation to the first category of cyberterrorism that targets public infrastructure, then the substantive law provisions of the 2001 Convention on Cybercrime ("CoC" also known as the Budapest Treaty), which was adopted in Articles 31 to 37 of Law No. 11 Year of 2008 concerning Information and Electronic Transactions ("UU-ITE"), in principle, can be used to prevent and overcome it. The activity of illegal access is regulated in Article 30 [8] illegal interception is regulated in article 31,[9] inter-

[8] Article 30 (1), (2) and (3) of UU ITE covers 3 (three) categories of illegal access actions each with a different penalty. The first category is intended for illegal access actions are only the beginning, usually made of investigations weakness of the system (vulnerability) with no authority or with bad intentions, for example, is an act against a system scan. The second category is the act of illegal access with the aim of obtaining information without authority, while the third category is illegal access actions undertaken by the destruction of the security system. In accordance Article 46 (1), (2) and (3) sets out the spectrum of penalties, ranging from a maximum of 6 years imprisonment and / or a fine of 600 million rupiahs up to a maximum of 8 years imprisonment and / or a fine of 800 million rupiah.

[9] Article 31 (1) and (2) recognizes the existence of two types of interception that is done for another person within the scope of the internal network (in a network) and external electronic systems in the network, either causing change or not resulting in changes to data. According to Article 47the penalty is 10 years imprisonment and / or a fine of 800 million rupiah. Article 31 (3) and (4) provide exceptions (primary justification) if the conduct is done by law enforcement officers for law enforcement purposes, so long as there is no misuse of authority.

ference of data is regulated in Article 32 [10], system interference is regulated in Article 33 [11] and the misuse of devices is regulated in Article 34 [12]. Trends suggest that cyber terrorism will, most likely involved is an act of vandalism or interference with data and / or tampering or interference actions that will lead to the disabling of system data and/ or electronic systems that are critical for the public.

As for the second category of cyber terrorism, which is dissemination of information for terrorism purposes, there are also several provisions UU ITE which can be used, namely Article 27 to Article 29[13]. In particular Article 27 (4) prohibits the disclosure of information that is blackmail or threatening mail[14]; Article 28 paragraph (2) prohibit the disclosure of information that is intended to engender hatred or hostility based on racism or racial intolerance (xenophobia)[15]; and Article 29 bans the transmission of information that contains threats of violence or personally addressed threats [16]

---

[10] Article 32\ (1), (2) and (3) 3 (three) categories of data interference, which are interference l within the scope of the network and interference at outside the network, and interference carried outagainst information that is confidential. According to Article 48, the third category is liable to imprisonment ranging from a maximum of 8 years and / or a fine up to 2 billion rupiah with a maximum imprisonment of 10 years and / or a fine of 5 billion rupiah.

[11] Article 33 only provides one category regarding system interference , either does not cause a serious damage or, widespread and causes widespread serious damage . The difference this classification will be determined later based on the implications of the article which gives weighting 1 / 3 of penalty points if the object is a public service, or a weighting of 2 / 3 if the threat to strategic state data or systems . According to Article 49 basic penalty is imprisonment for 10 years and / or a fine of 10 billion rupiah.

[12] Article 34 UU ITE imposes penalty on anyone who makes, provides, or has a device (either hardware or software following data content) whose aim is to only facilitate threatened criminal acts. It is also categorized on the act of abuse of a device. According to Article 50 , the penalty imprisonment for 10 year. and / or a fine of 10 billion rupiah. However Article 34 (2) provides an exception if the existence of these devices are intended for legitimate research, testing or for the protection of the electronic system.

[13] The authors opinion, the Article 27 (1) can also be used, if the judge agrees that "morality" can be applied in a broad sense, which would include not only pornographic material but also information about violence. In practice,however the Judge has tended to the meaning of decency in a narrow sense, which only the information relating to obscenity or pornography in violation of public decency standards.

[14] In accordance with Article 45 (1), the maximum penalty is imprisonment of 6 (six) years and / or a maximum fine of 1 billion rupiah..

[15] In accordance of article 45 (2), the maximum penalty is imprisonment of 6 (six) years and / or a maximum fine of 1 billion rupiah.

[16] In accordance of article 45 (3), the maximum penalty is imprisonment of 12 (twelve years) and / or a maximum fine of 2 billion rupiah.

In general, besides the Law of Terrorism and the UU – ITE that specifically apply to terrorism and cyber terrorism then a related enquiry is what is role, behavior and responsibilities of communications and media, in the context of the prevention and control of terrorism. Because, in the context of the dissemination of information on terror, the content is also contrary to morality and public order, and as a result we should consider legislation, such as: Law No.19 of 2002 Concerning Copyright ("Copyright Law"), Law No.40 of 1999 Concerning the Press ("Press Law"), Law No.32 of 2002 Concerning Broadcasting ("Broadcasting Law"), and Law No.39 Year 2009 Concerning Public Service ("Public Service Act") .

Article 17 of the Copyright Law clearly states that the Government prohibits any announcement contrary to Government policy in the areas of religion, defense and state security, morality, and public order after taking advice of the Copyright Board. Violation of this provision is subject to punishment under Article 72 (4) which states that whoever intentionally violates Article 17 shall be punished with imprisonment of 5 (five) years and/ or a maximum fine of Rp 1,000,000,000.00 (one billion rupiah). Until now, the writer has not seen any optimization of the function and role of the Copyright Board in an effort to prevent the spread of understanding of terrorism, or any guidelines to improve understanding. The writer also has not seen any movement from the Copyright Council.

Additionally, there is Article 5 (1) Press which states that the national press reporting incidents and is obliged to respect the norms of religion, have a sense of public decency and upheld the principle of presumption of innocence. Furthermore Article 18 (2) of the Press Law also states that a company violates provisions of Article 5 (1) must faces a maximum fine of Rp. 500,000,000.00 (five hundred million rupiah). Although the definition of the "press" covers electronic form (online), [17] the definition of media companies[18]is addressed only to Indonesian legal entities. Therefore, the application of the Press Law is limited to companies recourse against rather than the journalist / individuals using the internet for posting reports.

Meanwhile, the existence of a Press Council as an institution for public

[17] According to Article 1 (1) Press Law: The "press" is a social institution and mass communication, media journalism activities include looking for, acquire, possess, store, process and convey information both in written form, sound, images, sounds and pictures, as well as data and graphs as well as in other forms by using the print media, electronic media, and all types of channels available.

participation does not have the authority to set a community standard for press standard and content.[19]

Settlement with the mediation of the conflicted stakeholders' coverage must be filed by the parties themselves to the Press Council. A big question is if there is news about the terror that is no proportional, which any party is considered representative for taking it to the Press Council, as no class action mechanism is provided to the public under the Press Law. In addition, if there is a mistake in the reporting of a story it could prove it would be counterproductive and even lead to support for the terrorist. The writer has, up to now, not seen any active participation by the Press Council in preventing the danger of terrorism. At a minimum the Press Council should raise the discourse or examine how it could be preaching against terrorism.

In addition, there are also similar provisions relating to electronic media, Article 36 (5) of the Broadcasting Law, provides that prohibited to broadcast content if that content:[20] (a) is defamatory, inflammatory, misleading and/ or a lie; (b) highlight elements of violence, obscenity, gambling, abuse of narcotics and drugs; or (c) polarize ethnic, religious, racial, and pluralism (*antargolongan*). In addition, Article 36 (6) of the Broadcasting Law also states that it is prohibited to broadcast content that is parody, demeans, harass and/or ignores the religious values, dignity of Indonesian people, or damages international relations. Unlike the Press Council, the Indonesian Broadcasting Commission (KPI) holds more authority over con-

---

[18] Media companies are legal entities that conduct business in Indonesia and include print media companies, electronic media and news agency and other media companies that are specifically organized, broadcast, or distribute information (Article 1 (2) Press Law).

a. Protect press freedom from interference by other parties;
b. Conduct studies for the development of the press;
c. Establish and oversee the implementation of the Journalism Code of the Ethics;
d. Give consideration and seek resolution of complaints in cases relating to the press;
e. Improve communications between the press, public and government;
f. Facilitate press organizations in formulating regulations in the field of press and improve the professional quality of journalism; and
g. record company press;

[20] Article 1 (1) and (2) of the Broadcasting Law states that the Press is a message or series of messages in the form of voice images, or sounds and images or graphic form or character, whether interactive or not, that can be received through broadcast receiver device. While "broadcasting" is an activity of transmitting broadcast through transmission facilities on land, at sea or in space by using the radio frequency spectrum through the air, cable, and/ or other media to be received simultaneously by the community and the device.

tent that is broadcast,[21] however the law only applies to broadcast service providers (Radio and TV). Certainly it would be a thorny debate if the application of the Broadcasting Law was able to extend to the implementation of broadcasting via the Internet.

By way of comparison it is worth nothing as an example the way the Council of Europe Parliamentary Assembly, in Recommendation 1706 (2005) on Media and Terrorism requested the attention of media professionals to participate actively in the prevention and control of terrorism.

The Assembly invited media professionals:

i. to develop, through their professional organizations, a code of conduct for journalists, photographers and editors dealing with terrorist acts and threats, in order to keep the public informed without contributing unduly to the impact of terrorism;

ii. to organize training courses for media professionals aimed at increasing awareness of the sensitive nature of media reports on terrorism;

iii. to co-operate between themselves, for instance through their professional organizations, in order to avoid a race for sensationalist news and images which plays into the hands of terrorists;

---

[21] Article 7 (2)of the Broadcasting Law states that the KPI as an independent goverment institution regulate matters concerning broadcasting. Article 9 of the Broadcasting Law also states that:

(1) KPI should provide a basis for community participation and have a function to embody the aspirations and represent the interests of the community in broadcasting.

(2) In performing its functions as referred to in paragraph (1), KPI has the authority to:
  a. set standards for broadcast programming;
  b. develop rules and set the broadcasting code of conduct;
  c. oversee the implementation of regulations and codes of conduct and standards of broadcast programming;
  d. provide sanctions for breaches of regulations and codes of conduct and standards of broadcast programming; and
  e. coordinate and / or cooperate with Government, broadcasters, and the community.

(3) KPI has a duty and obligation to:
  a. ensure the public obtains information that is proper and correct in accordance with human rights;
  b. contribute regulating the broadcasting infrastructure;
  c. contribute to building climate of healthy competition between broadcasting and related industries;
  d. maintain the national information in a fair, equitable, and balanced manners;
  e. collect, examine and follow up complaints disputes and criticism and appreciation regarding the implemetation of public broadcasting; and
  f. plan human resource development that ensures professionalism in the field of broadcasting.

iv. to avoid acting in the interests of terrorists by adding to the feeling of public fear which terrorist acts can create or by offering terrorists a platform for publicity;

v. to refrain from publishing shocking pictures or disseminating images of terrorist acts which violate the privacy and human dignity of victims or contribute to increasing the terrorizing effect of such acts on the public as well as on the victims and their families; and'

vi. to avoid aggravating, through their news and comments, the societal tensions underlying terrorism, and in particular to refrain from disseminating any kind of vitriolic speech.

Meanwhile, in the context of telecommunications, Article 21 of the Law of Telecommunications states that telecommunications providers are prohibited to conduct telecommunication business activities that conflict with public interests, morals, safety, or public order. The elucidacion of this Article states that the the government can terminate the business license of such provider if based on the information obtained, it is strongly suspected or believed that the telecommunication organization has violated the public interest, morals, safety, or public order.

Article 38 of the Law of Telecommunications also states that every person is prohibited from engaging in acts that can cause physical and electromagnetic interference to a telecommunication network and those who violate (the provisions) referred to in Article 38 shall be punished with imprisonment of 6 (six) years and / or a fine of Rp 600,000,000.00 (six hundred million rupiah).

In the context of the Internet, the Ministry of Communications and Information cq Directorate General of Post and Telecommunications issued ministerial regulation No. 27/PER/M.KOMINFO/9/2006 concerning Telecommunications Network Security Based on Utilization of Internet Protocol that led to the formation of ID-SIRTII (The Indonesian Security Incident Response Team on Internet Infrastructure) as its governing body. The main task of ID-SIRTII is to provide technical support for the law enforcement process in the field of electronic transactions (Internet), for the security and monitoring of national Internet traffic and to provide an early warning against potential threats, attacks and harassment.

ID-SIRTII has been given authority to record transaction activities connections over the internet, monitor communication traffic on the Internet as

Multimedia Telecommunications Services and overcome or deal with problems, if for any reason, the functioning of the Internet is disturbed. It is unfortunate that the underlying paradigm is only limited to the security context of the functioning of the telecommunications channel instead of monitoring the information content and applications in the organization of electronic systems themselves. Therefore, the presence of ID-SIRTII actually still does not answer the mandate of Article 35 of the CoC regarding the 24/7 Network, especially the point of contact for the prevention and control of Cybercrime, particularly cyber-terrorism.

Article 35 – 24/7 Network

1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:
   a. the provision of technical advice;
   b. the preservation of data pursuant to Articles 29 and 30;
   c. the collection of evidence, the provision of legal information, and locating of suspects.
2. a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

   b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to coordinate with such authority or authorities on an expedited basis.
3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Considering all the existing legal provisions, the limitations can be seen by the existence and scope of application of the paradigm of regulation, which actually still not optimal nor comprehensive, and there is the existence of gaps in the prevention and handling of cyber-terrorism. This is because the various functions are still not optimal nor are the roles of the regulators for the purpose their professional responsibilities.

First, the Law of Terrorism, despite the provisions of the function and role of intelligence in counter-terrorism, has the only police to propelit, whereas intelligence efforts can also empower the state intelligence agency. The existence and scope of the intelligence authorities in Indonesia is still not yet well coordinated, because until now there has been no legislation addressing the State Intelligence. It would be better of course if the intelligence function involves not only police but also other elements as such as the Army of Indonesia Republic (TNI) in order to become more comprehensive. If the law-making process is long, the writer thinks the President can make a regulation (Perpu) for function and role of intelligence to involve all components agencies to become more coherent and comprehensive in preventing and tackling terrorism.

Interrelated with the functioning of the media, both in printed form and electronic, clearly there are limitations is that agencies cannot meet in supervising the implementation of the electronic system via the Internet. Meanwhile, in the context of the implementation of multimedia telecommunication services based on the implementation of telecommunications services based packet-switching and / or Transmission Control Protocol / Internet Protocol (TCP / IP), the new rules are a derivative of the Law of Telecommunications only, so it is limited in the security paradigm implementation of the pipe or channel of communication only. These provisions do not optimize the function role and responsibilities of Internet Service Providers (Liability Intermediary Services) in the conduct of law enforcement on the content and electronic systems.

The last hope really is to rely on the UU ITE, especially the Article 40.[22] The efforts of the Government to try to make the implementing regulations encompass multimedia content on the Internet (Draft of Ministerial Regulation concerning Multimedia Content/ RPM Konten Multimedia) should get a positive response for societies. But, unfortunately, the RPM is just a misunderstanding by the opposition due to certain people who already carried the opinion that these regulations will only suppress freedom

---

[22] In Article 40 UU-ITE, stated:

(1) Government to facilitate the utilization of Information Technology and Electronic Transactions in accordance with the provisions of legislation.

(2) The Government protects the public interest from all types of interference as a result of misuse of Electronic Information and Electronic Transactions of disturbing public order, in accordance with the provisions of legislation.

of opinion and are contrary to the principles of democracy. They are very worried that there is accountability for defamation on the Internet that has been relied upon as an alternative source of information as freely.

It is something very wrong and misleading that all information that passing on the Internet is said to be a part of the freedom of information and communication. Most of the businesses affiliated with the media will certainly have such thoughts. However, as a category which includes content that is against the law (unlawful content / illegal content) is not only a real person writing critical opinions but content may take the form of pornography, gambling, harrasment, blasphemy, racism, terror, unlicensed digital works, and so forth. It is unfortunate that public space was managed by the media capitalism in the name of "public trust" does not provide a balanced mechanism space to address or balance this issue.

In the context of the communications industry, the real parties that have business as a "service provider" have the technical control over every action, such as the sending and receiving information through electronic systems which is part of their business. They actually function as a means or can be said to provide assistance to these communications, either as a transmitter, forwarder, storage or those who rent the place (web-hosting) or even as a publisher of that illegal content. In the context of the implementation of global copyright, the mandate of Internet Service Providers (ISP) Liability is accommodated by a mechanism known as a "notice and takedown policy" against the illegal distribution of copyrighted works on the Internet. The service provider should not be considered responsible if they did not know the technical content. However, they still have to take responsibility if there are complaints or reports from the public, [23]

The substance of the provisions of the draft of Ministerial Regulation concerning Multimedia Content/ RPM Konten Multimedia, essentially only mandates what parties are responsible for the content (content owner or even service provider) and what to do if there were any reports or complaints relating to the existence of illegal content. On the other hand, RPM Konten Multimedia is provides a defense for the ISP in the face of lawsuits for Illegal actions (tort) or demands an inclusion of the spread of illegal

[23] Timothy D. Casey, ISP Liablity Survival Guide: Strategies for Managing Copyright, Spam, Cache, and Privacy Regulation., New York: John Wiley & Sons Inc., (2000)., hal .111.

content on the Internet. RPM Konten Multimedia can be a guideline for the ISP or to act as a Safe Harbor (secure area) for the ISP, because it will become a standard measure of the extent of the good faith to the ISP implements the duty of care in carrying out its duty the best efforts.

The urgency to carry out "blocking and filtering" is also reflected in the procedural aspects of the law of the CoC. In the context of child pornography, sexual intercourse between adults and children is an event that is naturally prohibited. Therefore, that kind of information that is prohibited abinitio should not be allowed to be viewed or stored by anyone. At the time the information is read or viewed by the public this immediately infringes the interests of child protection. So to prevent the dissemination an agreement is needed to perform blocking and filtering of illegal content.

Based on the above, it was clear that blocking and filtering policy are not only necessary for the purposes of copyright enforcement, but can also be applied to the prevention of terror, even to child pornography and other crimes. Having policies to carry out "blocking & filtering" is a necessity where electronic systems that open and free. It is not surprising that developed countries are more democratic and also have provisions to protect democracy itself.

Ironically, Indonesian government appears somewhat afraid to exercise the administrative authority. This may be a result views public interest groups / lobby groups of voiced by the media and by the existence of certain group pressure on social networks (examples: facebook and Twitter), whereas the larger society is in need of protection against the public norm.

It is unfortunate that community members do not agree with more comment, while, ironically, conservative society prefer to remain silent (silent majority) and form a movement. The strangeness is more prominent when there is an opinion and the motion stating that the concept is still a draft regulation should be revoked minister declared by the government, whereas the public test is being conducted in good governance form the framework of harmonizing all the existing public interest, not to dictate a democratic that just dominated for certain social groups.

Instead of participation that could be facilitated by laws, we also hope for the religious community participation, particularly the Uelama Council ("Majelis Ulama Indonesia"/MUI) that could also actively participate to counter the misuse of Islamic religions for terrorist purposes. They can enlighten people to understand the messages of Jihad as it is unwise to quote some articles of the Holy Quran without a comprehensive basic understanding of the subject matter. The biggest Jihad is how to handle human passion itself. Almost all of Indonesian Ulama teach the people how to follow Mohammad is behavior to give a peace not only for humanity but also the universe.

IV. Several Cyberterrorism Cases In Indonesia

In addition to the various bombing incident, the Indonesian people have also learned about cyberterrorism from at least two cases of misuse of the Internet for terrorist purposes, namely the "terror email" case and the case of site development for the dissemination of information terror.

The first case involved sending terror emails by the person charged to ex-boyfriend who married another woman by running to the United States. Due to heart problem, the person/ perpetrator has been sent an email with another name to the brothers of her former boyfriend, and also to schools and churches where the marriages will be held.

While the second case of site development for disseminating information about terrorism (www.anshar.net). Involved site used to communicate between terrorist and to also teach Internet users how the terror was carried out.

In the first case, besides charges occurring under Articles 336 and 335 (1) of the Criminal Code, charges were also made under Article 7 Law of Terrorism, which applies to everyone who intends to terror causing widespread fear. Meanwhile, in the second case, (registered as Case No. PN 84/ PID/B/2007 SMG), prosecutors have applied Article 13 (c) of the Law of Terrorism which applies to anyone who provides assistance or facilitates terrorist crimes, especially in this context, communication on the Internet.

V. Some Problems In Law Enforcement and Corrective Actions For the Future

Looking at what is occurring in law enforcement in these cases, and by looking at the legal dynamics that happen, here are some conclusions:

- Actions to prevent and control terrorism should not simply the Police, it also requires the active participation of the parties who have contributed and the ability to control and to counter the dissemination of information on terror,

- Although there are provisions which enable electronic information to be used as evidence, it still worth noting that the acquisition and securing of evidence and examination of electronic (digital evidence) to thetrial was not an easy task and law enforcement must consider the interested questions of privacy, good public service, and guarantee data integrity. The hharmonious coordination between the police, prosecutors and courts to expedite the good law enforcement is needed to make arrests and detain suspects and in order to conduct a search and seizure of electronic information.
- Although it is possible to receive intelligence information in the process of investigation, but unfortunately the legal system of Indonesia does not provide the intelligence institutions of Indonesia with a specific authority to tap individuals or business to facilitates intelligence there is no law for "intelligence"). The law of Terrorism contains special provisions concerning the protection of human rights of suspects/accused (so-called "safe guarding rules"). These provisions include introducing new legal institutions in criminal procedural law, called the "hearing" and serves as the institution of "legal audit" of all documents or intelligence reports submitted by investigators to determine whether or not forward with an investigation into allegations of acts of terrorism.
- Knowledge and confidence of judges in deciding cases still needs to be improved in order to identify and understand how the legality and validity of electronic evidence in court.
- Protection of witnesses seems suboptimal and the presence of any witnesses or expertwitnesses are vulnerable to intimidation from groups that might be pro-terrorism.
- Along with the utopia of freedom on the Internet, where experts could protest media UU ITE Article 27 because it is considered contrary to the guarantee of freedom of expression and opinion on the Internet. Many internet users could be object to the possibility of attempts to shut down a site, even if related with terrorism. Whereas in the context of domain name registration only, the provisions of the Uniform Dispute Resolution Policy (UDRP) was made possible existence of an attempt to suspend a domain name if its existence is not based on legitimate interests.

Interrlated with the matters, based on recent information, The Ministry of Communication and Informatics ("Kominfo") cq Directorate General of Telematics Applications in cooperation with the National Law Development Agency (BPHN), is working hard to prepare the draft of law for acceding to the Convention on Cybercrime and the Criminal Acts in IT (Draft of TIPITI) the substance of which will complement the of UU ITE. Inside the Draft of TIPITI some things that are not yet regulated in UU ITE, especially the procedural law and following mutual cooperation (mutual legal assistance). The presence of a specific provision of the following cyber terrorism and possibility the closure of terrorism-related sites should also be considered, if it is needed.

VI. Conclusion

Until now, although the police seem to be relatively successful in approaching terrorists, we should still continue to walk towards optimizing the role of the dissemination of terrorism information dissemination on the Internet. Although the Law of Terrorism and the Law of Information and Electronic Transactions (UU ITE) can be used to capture the perpetrators of cyberterror, the provisions of other relevant laws, should also be developed more in order to provide a space for stakeholders to actively help prevent and combat terrorism. Even though the government has made ID-SIRTII as a security guard internet network, the role of the Internet Service Providers, media players and community institutions should continue to play an important role in the future.

When compared to other countries where the role of intelligence is also proposed to prevent terrorism, Indonesia seems to still optimize it may be possible because of fears of the past, where the state intelligence has been used to perpetuate power. While the reform is taking place, of course, the State Intelligence need sufficient authority to assist law enforcement authorities, particularly in crime prevention against terrorism. As the history has told us, the harmonious cooperation between law enforcement and intelligence is the key country to preventing crime of a a transnational nature.

As a final note, the efforts to prevent and control terrorism, especially within the scope of the Internet, should be getting attention and a shared commitment from all stakeholders, so as to ensure of Indonesia's future is safe, peaceful, just and prosperous.