ATLANTIS PRESS

Advances in Social Science, Education and Humanities Research, volume 162

International Conference on Law and Justice (ICLJ 2017)

Cyber Child Pornography

Law and Technology Problems in Its Law Enforcement

Agus Raharjo
Universitas Jenderal Soedirman
Jl. Prof. dr. Boenyamin 709, Grendeng, Purwokerto, Indonesia
agus.raharjo007@gmail.com

Abstract*—Rapid grow of internet users as a result of widely open access significantly contributes to increasing criminal cases particularly child pornography. Internet becomes a convenient place for users to commit distant crime by accessing porn images or child photographs as well as child sexual activity. Meanwhile, current methods to prevent and solve are considered ineffective and conventional. This paper discloses the increasing number of child pornography and provides solution to overcome it. It applied juridical, normative, empirical and technological methods. The results show that it is a tough task for law enforcement officials to find, detect and put the child pornography offenders in prison. The given law is too child-oriented, that is, it contradicts imprisonment concept to put children in jail. Thus, other form of imprisonment is needed including limited access, prohibition and access supervision for the perpretators. Yet, a question follows: who will supervise the access? A set of regulation is then seemingly required. Technology utilization expectedly can contribute to prevent child pornography in terms of software, filter or detector. Considering technology failure few years ago, technology advancement need maintaining to block creativity of cyberchild pornography to hack the information system to reach their goal.*

Keywords—Cyberchild Pornography; Information Technology; Internet; Cybercrime; Juvenile Justice;

I. INTRODUCTION

Pornography is a business sector that continuesly develops, even when this country faced monetary country. In the last two decades, pornography business received quick commercial success. However, not every country could obtain the profit of this business. Only several countries that are able to gain the profit particularly countries with no strict regulation on morality. U.S. is country that mostly gains profit from this business. It is the country which produces more than 150 titles of hard-core films or videos per week. U.S. also receives income from sex magazines selling, Internet porn, phone sex businesses, peep shows, and adult cable programming. In all, the industry grossed eight billion dollars in 1996, more than the entire receipts from all Hollywood's movies put together (Fisher and Barak, 2000; Thio, 2001). Observers of cyberporn have speculated that the growth in its popularity is linked to the three ''As'': accessability, affordability, and anonymity (e.g., Putnam 2000; Stack, et.al, 2004). Therefore, there is prohibition on pornography, and its trade is considered as illegal in Indonesia. Moreover, the commercial value of this business cannot be known certainly.

If the behavior and regulation of adult pornography are different in each country, then almost all countries have similar standpoint in child porno-graphy.. The danger of child exploi-tation and the protection of their future are several cosiderations why it is prohibited. The existence of website containing child pornography causes anxiety to each child, parents, government, and also state.

The advance of computer technology with its variants like desktop, laptop, android, and hand phone which are connected to the Internet offers access to world wide webs that provide pornographic contents. The worry on cyber child pornography must be paid attention since BBC News (2001) had indicat-ed the existence of that matter in Indonesia. Since about 2000, international coalitions of law enforce-ment agents have worked in a similar manner to crack down on international cyber child porn rings. A major case in point occurred on August 8, 2001, when U.S. legal authorities arrested over 100 people for sub-scribing to an Internet site blatantly selling child porn. Authorities then said that they had cracked the largest child porn ring ever discovered. The Internet Website had more than 250,000 subscribers and was run from Texas, through operations in Russia and **Indonesia**. The child porn was also distributed through regular post (Schell, et.al, 2007). It seems like Indonesia has become international player in distributing cyber child pornography. This is a serious problem.

Reflecting from wonderland case which was horrendous in Eropa and America, Indonesia must have self-improvement in dealing with the production and distribution of cyber child pornography. Besides categorized as the country which operates the site with pornographic contents, Indonesia also becomes the destination country of pedophiles. It is proven by the case of Australian tourist who was prohibited to visit Bali because that person was indicated as a pedophile. This paper discusses the regulation on cyber child pornography and its law enforcement as well as offers breakthrough in its investigation process.

This research is a qualitative research with normative juridical approach and a research on law in action. It is social science which is non-doctrinal and empirical. The data source in this research is humans with their behavior, event, document, archives and other things. The data are collected by

using interactive and non-interactive methods. The data obtained are analyzed by applying interactive analysis model.

II. The Regulation on Cyber Child Pornography in Indonesia

The sexual harassment cases toward children in 2016 triggers the government to issue Government Regulation Substituting Law Number 17 Year 2016 which then become Law Number 1 Year 2017 on Determination of Government Regulation Substituting Law Number 1 Year 2016 on The Second Amendment of Law Number 23 Year 2002 on Child Protection become the Law. Beside adding new action as criminal act, the matter which then causes contro-versy is the existence of regulation regarding castration law and the installation of electronic detector for perpetrators against children (Article 81 paragraph (7)). Even though the detector is not directly pointed to the perpetrators of cyber child pornography, this regulation seems like giving serious impact to them.

The specific regulation regarding cyber child pornography in Indonesia has not existed yet. Never-theless, there are several regulations related to children and pornography in various laws. The core of regulation regarding pornography exists in Law Num-ber 44 Year 2008 on Pornography. In this law, porno-graphy is defined as picture, sketch, ilustration, photo, written from, voice, sound, moving picture, animation, cartoon, conversation, body movement, or other forms of message through various communication media and/or the show in public which contains obscenity or sexual exploitation that breaks morality norm in so-ciety (Article 1 paragraph 1).

In article 4 of this Law , there are two categories of prohibitions in pornography, that is:

A. *Every person is forbidden to create, fabricate, commercial quantity duplicate, reduplicate, spread about/distribute, broadcast, importation, ex-portation, make for sale, trade in, lease/rent, prepare/make available or store/lay-away pornography which has the following traits:*
    1. coital acts, foreplay and sexual diversions pertaining to coitus;
    2. sexual violence;
    3. masturbation or onanism;
    4. nudity or illusions/allusions to nudity;
    5. genitalia; or
    6. child pornography.

B. *Every person is forbidden to set aside/prepare porn which:*
    1. depicts explicit nudity or illusions of nudity;
    2. depicts explicit genitalia;
    3. exploitational or pedantic allusions to sexual activities; or
    4. make or advertise in sense of commercialized publications in spite of no relation to sex.

Other prohibition in this regulation is: to borrow or download pornographic content (article 5); listen, watch/view, utilize/exploit/employ, possess, or store/have in storage porno-graphy product (article 6); to facilitate deeds as defined in article 4 (article 7); intentionally or upon his/her consent to be an object or pornography model (article 8); to make another person an object or porno-graphic model (article 9); and to view personally or exhibit/perform in the general public nude depictions, exploitation of sex, coital acts, or other that alludes to pornography (article 10).

This regulation does not give definition and specific regulation about child pornography. It only regulates the prohibition of child involvement in pornographic criminal act as set forth in article 4 to 10 (Article 11) and child protection from the influence and access to pornography (Article 15), as well as the imposition of obligation to government, social institu-tions, educational institutions, religious institutions, family, and/or society in founding, accompanying, and recovering social condition, physical and mental health of each child who becomes the victim or pornography doer (Article 16 paragraph 1).

Referring to the use of the internet network for cyber child pornography activities, minimum regulation on this subject is found in, namely Article 52 para-graph (1) *juncto* Article 27 paragraph (1) *juncto* Article 45 paragraph (1) of Law Number 11 Year 2008 on Information and Electronic Transactions. The main article of the arrangement of this issue, Article 27 para-graph (1) only regulates the activities of distributing and/or transmitting and/or making accessible Electronic Information and/or Electronic Documents that have content that violates morals. The widely stated meaning of this decency is interpreted to include cyber child pornography when it involves a child in it (Article 52 paragraph (1) with the threat of a third of the principal penalty as threatened in Article 45 paragraph (1). An arrangement similar to the ITE Law concerning the prohibition committing acts that violate morality can be found in the Telecommunication Law, Broadcasting Law, and others, without further regulation of the involvement of children in it.

The absence of a clear definition of cyber child pornography or child pornography causes its definition to refer to the notion of pornography in general as it appears in pornography laws. The problem is not only the use or insertion of the word "child" in the legislation, but also the material or criteria used may be different. Child pornography is not an easy concept to be defined and that tension will always arise between the desire to criminalize exploitative material and personal freedom such as expression and free speech (Gillespie, 2010). Since there is no definite definition, the understanding of the legislation of other countries can be used as consideration in determining or defining cyber child pornography in the future.

U.S. Federal law on child pornography, on article 18 U.S.C. § 2256 provides definition of child pornography. Child pornography is a form of child sexual exploitation. Federal law defines child pornography as any visual depiction of sexually explicit conduct involving a minor (person less than 18 years old). Image of child pornography is also referred to as child sexual abuse image. Federal law prohibits the production, distribution, importation, reception, or possession of any image of child pornography. A violation of federal child pornography laws is a serious crime, and convicted offenders face fines severe statutory penalties (Magid, 2002).

Other definitions can be cited from Canada. The Criminal Code now defines "child porn" as "a photo-graphic, film, video, or other visual representation, whether or not it is made by electronic or mechanical means ... that shows a person who is or is depicted as being under the age of 18 years old and is engaged in explicit sexual behavior ... or the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region under the age of 18 years ... or any written material or visual representation that advocates or counsels sexual activity with a person under the age of 18 years ... "(Department of Justice Canada, 2002).

The legal system attempts, through actual legislation and grades sentencing policy, to control child pornography. The function of law needs to be more carefully defined so as to focus more clearly on child protection and on the surest means of delivering this (Williams, 2004). Although there is no principal difference between these definitions and the general definition of pornography laws, the existence of strict regulations regarding cyber child pornography will have implications for law enforcement.

III. Law Enforcement of Cyber Child Pornography in Indonesia

Cyber child pornography is part of cybercrime, which has distinctive characteristics that require different handling with pornography in general. Law enforcement within the cybercrime prevention framework reacts in much the same way as traditional crime deals. The internet and the criminal behavior it transforms (cybercrime) pose considerable challenges for order maintenance and law enforcement because Internet-related offending takes place within a global context while crime tends to be nationally defined. Policingcybercrime is more complex by the very nature of policing and security by networked and nodal and also because within this framework the public police play only a small part in the policing of the Internet (Wall, 2007; Wall and Williams, 2013).

Traditional crime has scope, scale, time, and limited space, so law enforcement can react quickly to it. Whereas cybercrime - as introduced by Brenner - has characteristics that are different from traditional crimes in several ways, namely: first, though it is carried out by a small percentage of the population of a society (or of the world, since cybercrime tends to ignore boundaries), a relatively small group can commit crimes on a scale far surpassing what they can achieve in the world where one-to-one victimization and serial crimes are the norm. Consequently, the number of cybercrimes will exponentially exceed real world crimes. Second, cybercrime is additional to the real-world crime with which law enforcement must continue to deal; people will still rape, rob, and murder. These two factors are combined and create an overload; law enforcement's ability to react to cybercrime erodes by cyber-crime and real-world crime together (Brenner, 2008).

This is the fact that causes cybercrime differ from traditional crime and its law enforcement. The traditional reactive mode is not effective for cyber-crime, because cybercrime is elusive. Offenders are elusive because there is no necessary nexus between the site of a 'crime' is committed or afterward. They are also elusive because they can shield their identities and avoid leaving the traditional types of physical eviden-ce. "Crimes" are elusive because they do not fall into recognizable offenses and/or offender patterns and be-cause they can be committed on such a scale that law enforcers simply cannot react to all of them (Brenner, 2004).

There are two models in the investigation of criminal cases, namely crime control model and due process model. Both have significant disadvantages in the cybercrime prevention and control process. Crime control models or reactive models, as they are known in criminal justice and committed by police, are not ef-fective enough to prevent cybercrime. Reactive strate-gies for cybercrime cannot be properly implemented because once the crime has been committed, the offender can remove the trail easily. Moreover, these crimes occur in an electronic environment, so that the physical evidence is easily lost from memory, or evidence can be easily destroyed. The police may be able to determine the location where the offender accesses the internet after tracing the activity through log files, but when examined it may be that the offender has gone or instead uses anonymity where it is possible in cyberspace. In other words, the use of formal activities (affirmative model) is not suitable to handle cybercrime (Raharjo, 2013).

The Internet has distinctive features that shape the crimes that take place in cyberspace. These features pose difficulties for tackling crime when approached by established structures and processes of criminal justice systems. Not least among, these is that policing has historically followed the organization of political, social and economic life within national territories. Moreover, crime control agencies like to focus their attention and resources on crime occurring within their 'patch'. Yet, cybercrime, given the global nature of the Internet, is inherently de-territorialized phenomenon. Crimes in cyberspace bring together offenders, victims and targets that may well be physically situated in different countries and continents, and so the offenses span national territories and boundaries (Yar, 2009).

It is said by Brenner that for the current law enforcement model - which makes the process of reacting to crimes (or cybercrimes) the exclusive province of a cadre of government-sponsored, professional law enforcement agents - is not, and will never be, adequate to keep cybercrime and related evils such as cyber terrorism within acceptable bounds. Indeed, the problems we are using are migratory from the "boxes" we currently use and embed itself into our environments and, perhaps, into ourselves (Brenner, 2007).

Similarly, the due process model is not suitable to complete cybercrime completely. The typology of due process model with the negative model always emphasizes the limitation on formal power and modification of the use of power, where the dominant power in this model is the judicial power and always refers to the constitution. In Indonesian criminal justice, the judicial power is in court, and it is said to be the final wall of justice, whereas cybercrime cannot be quickly prevented through courts of tortuous proceedings. This model is suitable for legal certainty, but not suitable for preventing crime, let alone types of crime that have high speed and mobility rates such as cybercrime (Raharjo, 2013).

Based on an explanation of the above models of crime prevention and overcoming, it can be further argued that the model of law enforcement we currently rely upon is not effective in dealing with cybercrime, at least, is not as effective as it needs to be to control the incidence of cybercrime. The current model is not effective because, reasonably enough, it was develop-ed to deal with real-world crime. As a result, it incorpo-rates (i) certain assumptions about crime and (ii) cor-relative assumptions about how law enforcement reacts to completed crimes in a manner that sustains the level of deterrence needed to keep crime under control. The model is not effective against cybercrime because the assumptions it makes about crime do not hold for cybercrime: Unlike crime, cybercrime is routi-nely transborder/transnational in nature, which means there is usually not a single, localized crime scene that becomes the focus of an investigation; and because it is automated, cybercrime is routinely committed on a scale vastly exceeding the scale on which it is possible to commit crimes. Singly and in combination, these factors create challenges for law enforcement's inves-tigatory procedures and resources (Brenner, 2004).

In addition to the difficulties caused by incom-patibility of the cybercrime prevention and control model in the criminal justice system, other issues actually arise along with the distinctive characteristics of cybercrime that are not the same as traditional crimes, either from deeds, means, or ways of dealing with them. Yar wrote that further problems arise when we consider the constraints of limited resources and insufficient expertise. Lack of appropriate expertise also presents barriers to the effective policing of cybercrime. Investigation of such crimes will often require specialized technical knowledge and skills, and there is at present little indication that police have the appropriate training and competence. Moreover, re-search indicates that many police do not view the in-vestigation of computer-related crime as falling within the normal parameters of their responsibilities, under-mining attempts to put such policing on a systematic footing (Yar, 2009).

The difficulties are further intensified once we consider the problem posed by different legal regimes across national territories. The move toward interna-tional harmonization of Internet law has already been noted. Yet such developments are in a relatively early stage. Examination of Internet law reveals that many countries lack the legislative frameworks necessary to effectively address Internet-related crimes. Attempts to legislatively tackle cybercrime may also run foul of existing national laws. Even where appropriate legal measures have been put in place, many countries (especially in the 'developing world') simply lack the resources needed to enforce them. In countries facing urgent economic problems, with states that may be attempting to impose order under conditions of consi-derable social and political instability, the enforcement of Internet laws will likely come very low on the list of priorities, if it appears at all (Yar, 2009).

Based on the existing weaknesses of the exist-ing crime prevention model, new steps are needed, as it prevents cybercrime (cyber child pornography) from more than just legal or technical matters, not just the police duties but also the tasks of stakeholders utilizing the Internet (Internet Service Provider), parents, com-munity and government. The police are not a faithful god of help at all times be there at the crime scene, in fact, often he is always left with the crime itself. In other words, the crime had run faster when the police arrived at the scene.

The need for a new approach in cybercrime prevention is based on three premises as stated by Brenner. Our need for a criminal law of cyberspace derives from three premises, the first of which was derived above: it is already apparent that the traditional model of law enforcement, with its reactive approach and hierarchical, military-style organization, cannot deal effectively with cybercrime. The second premise derives from the proliferation of technology. Technology – in the form of computer, personal digital assistants, cellular phones, mobile entertainment devices, pager, Global Positioning System gear and other appliances – pervades much of our daily life, at least in more developed countries. This tendency will only become more pronounced ad wireless communication technologies, sentient chips, wearable computers, smart rooms, digital cities and other techno-component of life transform our environment in the twenty-first century. The proliferation of these devices, all linked in various and varying ways, will create and sustain a fluid, continuously operating global network (Brenner, 2004).

This takes us to the third premise: the proli-feration of these technologies will have a profound effect upon the organization of human social systems and activities. As noted above, the world will become a single interdependent, interlinked network. For the last several millennia, the organization of human social systems and activities – government, commerce, edu-cation, religion, military – has been hierarchical: a top-down approach to the structuring of social relationship and the allocation of authority. This default hierarchi-cal organizational model evolved to deal with the organization of activity in the real world. since human activity is subject to the physical constraints of empi-rical reality, it requires the use of techniques such as a chain of command to orchestrate and focus the efforts of groups of humans on achieving particular tasks, e.g., mining coal, smelting steel, sailing ships, building pyramids, waging wars and keeping order within a social system (Brenner, 2004).

The Internet puts us in no hierarchy as in an or-ganization, can be anywhere, which forms a new type of social organization, the network. When a hierarchy places a person in proportion in a social organization, then in a network it smashes the boundaries, tears down the hierarchy and dismantles the bureaucracy (Lipnack and Stamps, 1994). Networks, unlike hierarchies, are lateral, fluid systems, decentralize power and authority, and thereby empowering individuals. Networks have the capacity to, and very likely will, usher in a new era of cooperation among peoples and among social systems. Unfortunately, they can also be exploited for destructive purposes (Bren-ner, 2004).

There are several alternative solutions that can be given. *First*, adding police pesonil to be able to react quickly to the occurrence of cybercrime. The assum-ption is that with increasing personnel, the speed at handling cybercrime can increase. There is an oblique view of the police, where the view of one of the duties of the police, ie preventing crime, is considered a myth. Police do not prevent crime. This is one of

the greatest secrets in modern life. The experts know it, the police know it, but the public does not yet know it. But the police pretend they are the best protectors of society from crime and always say if given more resources, especially personnel, they will be able to protect society from crime. It's just a fairy tale (Raharjo, 2013; Bayley, 1998). Therefore, what needs to be done is that the police must change the way of thinking. It is suggested that there is currently in the appreciation of how the internet (social media) is impacting upon the new technologies, the internet has the potential to transform many policing practices more quickly (Goldsmith, 2015).

Second, the formations of cyber police or cyber cop, which specifically deal with cybercrime problems and can quickly react if there is an incident, be equipped with modern structure and infrastructure internet. Cyber cop is not necessarily human, but it can also be automatic policing in cyberspace. About this, Brenner said, this would involve using automated agents to react to completed cybercrimes and to "patrol" public areas of cyberspace in an effort to prevent the commission of cybercrime. While automated cyberpolicing is certainly a logical alternative, its implementation is surrounded with technical and legal difficulties, thus making it an unrealistic option for the foreseeable future (Brenner, 2004).

According to Anglin (2002), law enforcement agents in the United States often engage in undercover operation that involve mailing child pornography to suspected consumers. The law enforcement agencies should alter their practices. In enforcing laws against the possession of child pornography, federal law-enforcement agencies engage in elaborate undercover investigations in which they mail pornographic images of actual children to suspected pedophiles. Thus, the current method of federal undercover child pornography investigations should be evaluated by the Attorney General's office, which should adopt new undercover law enforcement techniques.

A third alternative is to authorize civilian use of defensive technologies, i.e. to let cybercrime victims use "strike-back' or 'counterstrike' tools". The rationale here is that victims react when they are the targets of cybercrime and thereby supplement the reactive capabilities of law enforcement personnel. The premise is that a computer system which is 'under attack automatically traces back the source and shuts down, or partially disables, the attacking machine(s)". This alternative raises difficult legal question, but ulti-mately founders on the risks involved in authorizing victim self-help (Brenner, 2004).

Some of the above prevention models are based on territories with existing communities in real-world. Of course with such background and rationale, preven-tion by relying on the police and the victim cannot prevent cybercrime well. Then again, cybercrime is different from real-world, because cybercrime is a fluid, lateral phenomenon; it is, in effect distributed "crime". Since cybercrime is a lateral, pervasive phe-nomenon, it demands a lateral, pervasive solution. This solution can incorporate a reactive element, a purely reactive approach will be inadequate. The solution therefore needs to be proactive; it must focus on preventing cybercrime, not merely reacting to it. The solution also needs to employ collaborative approach, one that combines the efforts of civilians and law enforcement. this approach addresses the problem noted earlier namely that it is neither financially nor pragmatically possible to deploy enough law enforce-ment officers to maintain order in cyberspace. Therefore the way to address cybercrime is to utilize the community policing model's concepts of a proac-tive, collaborative approach to "crime" (Brenner, 2004).

This alternative prevention model is based on the internet user itself (prevention based by user). This means the foothold to prevent cybercrime is no longer the government, police or justice system but it will be the internet user. In a narrow sense, internet users should be equipped with knowledge about good ways to use internet (guidance principle using internet) or understand cyber ethic or netiquette. This step is referred to as prevention by defense by the users themselves that tend to arise. In addition, the user must also complete the Internet infrastructure with a security system that should be kept updated by keeping in mind that technological development happens very fast. (Raharjo, 2013). This model relies more on the user's sense of responsibility for themselves and more broadly for the people of internet security. This model places criminal law (along with its apparatus) on the right proportion, for example, as an ultimum remidium, by promoting public participation (Internet users) in crime prevention.

Another model introduced by Brenner is prevention law enforcement. This model gives power to the police or law enforcers to identify and take down people who may be able to do crime before they are able to do it. In other words, law enforcers take action before the proof is completed by doing intervention before the crime really happens. This makes it possible to law enforcer to intervene and take down individuals based on prediction over their potential in doing crime. Nevertheless, this model tends to count on one's indicator which appear on the surface, too general and tend to neglect the guarantee of legal process (Brenner, 2008). If this is implemented, it will be dangerous for law enforcer because they can be accused for misusing power and there will be many law enforcers who receive judgment (Raharjo, 2013).

Even though the burden for preventing crime through the model above has shifted to internet user, this does not mean legislation and judicial function (criminal justice system) is unimportant. These functions are still important since the pace of technology information development, especially internet, needs to be anticipated through regulations in legislation. Mc-Quede III (2009) writes that Internet carries with it significant new risks of criminal victimization, and thus present some pressing challenges for legislators and criminal justice agencies. However, attempts to police the Internet for the purposes of crime control also raise serious dilemmas and dangers. Central here is the tension between surveillance and monitoring of online activities, on the one hand, and the need to protect users' privacy and confidentiality, on the other. Law enforcement agents need to be able to identify offenders and collect evidence of online crimes. Offenders, however, are able to exploit anonymity and disguise to hide themselves and their activities from praying eyes.

Prevention based by user model requires user to know, understand and update to the development of information technology, especially technology for internet safety.

However, since there is limitation of user knowledge, several basic security systems should have been built up in the sold computer or laptop. In other words, this model emphasizes the importance of computer producer (business entity) to be responsible by participating in cybercrime prevention, even though this is not hierarchy like organization mentioned above. The users still have their own authority in deciding which security system installed in the computer.

There are various offers on prevention based by user model which mostly directed to development of software. Ministry of Information and Informatics has ever provided software freely to prevent pornography in general. Nonetheless, the development of this software has no further follow-ups. Prevention and legal instruments have also been used through regulation of Ministry of Information and Informatics on Trust+ which gives power to Ministry of Information and Informatics to close or block sites that contain pornography. However, this does not have maximal result.

The development of software which can prevent the use of internet to produce, save, transmit and distribute materials containing cyber child pornography should continue develop since pedophiles will not stay put and fight against this software which aim to prevent their activities. The suggestion from Schell et.al (2007) is worth to try. He stated that, "our technical approach to combating cyber child pornography consists of enhancing routers with a classification system combining the SLWE with a linear classifier. This classification system, along with a Bloom filter with counters which keep track of source IP address reputation…"

Child pornography crimes may involve multiple jurisdictions and cross-national borders. Therefore, this analysis suggests at least three implications for policy and law enforcement practice. First, there is a need for a more formal national and global infrastructure to support these investigations. Second, law enforcement agencies need additional resources, specifically allocated for assisting in expert witness or other assistance in ascertaining if images depict minor children. Finally, this analysis suggests that while law enforcement investigators report using innovative, technology-enhanced investigation strategies, the nature of the Internet appears to present significant challenges for law enforcement (Wells, 2007).

Difficulties in law enforcement against cyber child pornography is not only faced by Indonesia. America, England, Australia, Wales and the Netherlands experienced similar problems (Jewkes and Andrews, 2006). Cybercrime prevention requires a strategic national security. in the UK a renewed policy focus on cybercrime and information warfare, embodied within the Cyber Security Strategy. The UK develops Police Central eCrime Unit (PCeU). Europe has also established the European Cybercrime Center (EC3) at Europol in an effort to address transnational crimes (Wall and Williams, 2013). Since this crime is a transnational crime, international cooperation and regulatory harmonization need to be done. Therefore, the investigation in the judicial system on the cyber child pornography case does not exist yet, then the alternative problem solving offered above can be used by the courts in Indonesia.

Those efforts need to be followed by activities to catch and process pedophiles legally. Treatment is required for cyber child pornography users so that they can be healthy again, because they are not just criminals, but also psychologically ill (Seto, et.al. 2010; Middleton, et.al. 2006; Quayle and Taylor, 2002; Burke, et.al, 2002). There must be a cooperation done by law enforcer and people to save the next generation from early sexual exploitation.

IV. Conclusion

Treatment for cyber child pornography often faces failure caused by lack of knowledge related to the cause of the crime, the incapability of law enforcement apparatus, inappropriate education system, low participation from the people for law enforcement, and no development of software to prevent on an ongoing basis. Fighting against cyber child pornography requires a lot of strategy. *First*, the need to search basic or main reason for emergence of cyber child pornography; *second*, there should be a complete and clear rule on material and formal substances of cyber child pornography; *third*, there needs to be improvement on technical ability and tools for law enforcement apparatus; *fourth*, there needs to be improvement for participation of people; and *fifth*, there should be development of software continuously and easy access for internet users.

Acknowledgments

The researcher would like to express gratitude to some of the parties who have helped researcher during looking for data and finishing this paper. First and foremost, the researcher expresses thank you to Chair-man or Rector, Chairman of research institutes and community service, Dean of Faculty of Law, Jenderal Soedirman Universty. Also, thanks for my student, Suyogi Imam Fauzi, Inge Puspitaningtyas, Sri Wah-yuni, and Enamel Audha, which have been helpful in searching data. Hopefully the help given will receive a reply from Allah SWT.

References

[1] Anglin, Howard. (2002). "The Potential Liability of Federal Law-Enforcement Agents Engaged in Undercover Child Pornography Investigation". *N.Y.U Law Review*, Vol. 77, October. Pp. 1090-1118.

[2] Bayley, David H. (1998). *Police For The Future*. Jakarta: Cipta Manunggal;

[3] BBC News (2001, August 8). U.S. breaks child cyber-porn ring. Retrieved March 11, 2006, from http://news.bbc.co.uk/1/hi/world/americas/1481253.stm, access on 27th May 2014.

[4] Brenner, Susan W. (2004). Toward a Criminal Law for Cyberspace: Distributed Security". 10 *Boston University Journal of Science & Technology Law* 1.

[5] Brenner, Susan W. (2007). "Private-Public Sector Cooperation in Combating Cybercrime: In Search of a Model", *Journal of International Commercial Law and Technology*, Vol. 2, Issue 2, pp. 58-67

[6] Brenner, Susan W. (2009). "Distributed Security: Moving Away from Reactive Law Enforcement", *International Journal of Communication Law and Policy*, Special Issues Cybercrime Spring, pp. 1-43

[7] Burke, Anne. Shwan Soerbutts. Barry Blundell & Michael Sherry. (2002). "Child Pornography and the Internet: Policing and Treatment

Issues". Psychiatric, Psychology and Law, 9:1, pp. 78-94. DOI 10.1375/pplt/2002.9.1.79.

[8] Department of Justice Canada (2002, June 10). Highlights of Bill C-15A: An act to amend the Criminal Code and to amend other acts protecting children from sexual exploitation. Retrieved March 11, 2006, from http://canada.justice.gc.ca/en/news/nr/2002/doc_30531.html, access on August 24th 2010.

[9] Fisher, William, and Azy Barak. (2000). ''Online Sex Shops: Phenomenological, and Ideological Perspectives on Internet Sexuality.'' *Cyber Psychology & Behavior* 3:575–89.

[10] Gillespie, Alisdair. (2010). "Legal Definition of Child Pornography". *Journal of Sexual Aggression: An International, Interdisciplinary Forum for Research, Theory and Practice*, 16:1, pp. 19-31. DOI 10.1080/1355.2600903262097.

[11] Goldsmith, Andrew. (2015). "Disgracebook Policing: Social Media and the Rise of Police Indiscreation". *Policing and Society*, 25:3, pp. 249–267, DOI 10.1080/10439463. 2013.864653

[12] Jewkes, Yvonne & Carol Andrews. (2005). "Policing the filth: The Problem of Investigating Online Child Pornography in England and Wales". *An International Journal of Research and Policy*, 15:1, 42-62. DOI 10.1080/1043946042000338922.

[13] Lipnack, Jessica & Jeffrey Stamps. (1994). *The Age of the Network, Organizing Principles for the 21st Century,* New York: John Wiley & Sons.

[14] Magid, L. (2002, March 21). Net users can help fight child porn. Retrieved March 9, 2006, from http://www.pcanswer.com/articles/sjm_childporn.htm, access on 15th June 2014.

[15] McQuede III, Samuel C. (ed). (2009). *Encylopedia of Cybercrime*. Westport CT: Greenwood Press.

[16] Middleton, David. Et.al. (2006). "An investigation into the applicability of the Ward and Siegert Pathways Model of child sexual abuse with Internet offenders". *Psychology, Crime & Law*, 12:6, 589-603, DOI 10.1080/10683160600558352.

[17] Putnam, D. E. (2000). ''Initiation and Maintenance of Online Sexual Compulsivity. Implications for Assessment and Treatment", *Cyber Psychology and Behavior* 3, pp. 553–64.

[18] Quayle, Ethel and Max Taylor. (2002). "Child Pornography and the Internet: Perpetuating a Cycle of Abuse". *Deviant Behavior*, 23:4, pp. 331-361. DOI 10.1080/01639620290086413.

[19] Raharjo, Agus. (2013, June). Pencegahan Cybercrime Melalui Pengembangan Prinsip Pertanggungjawaban Pidana Bagi Pengguna Internet, *Paper* on Seminar Nasional Hukum Pidana, Purwokerto.

[20] Raharjo, Agus. Angkasa, and Hibnu Nugroho (2013). "Rule Breaking dalam Penyidikan untuk Menghindari Kekerasan yang Dilakukan oleh Penyidik". Jurnal Dinamika Hukum, 13:1, pp. 59-74.

[21] Schell, Bernadette H.; Miguel Vargas Martin, Partick C.K. Hung, Luis Rueda. (2007). "Cyber child pornography: A review paper of the social and legal issues and remedies – and a proposed technological solution", *Aggression and Violent Behavior*, 12, pp. 45-63

[22] Seto, Michael C. Lesley Reeves & Sandy Jung. (2010). "Explanations Given by Child Pornography Offenders for their Crimes". *Journal of Sexual Aggression: An International, Interdisciplinary Forum for Research, Theory and Practice*, 16:2, pp. 169-180. DOI 10.1080/13552600903572396.

[23] Steven Stack, (2004). Ira Wasserman, and Roger Kern, "Adult Social Bond and Use of Internet Pornography", *Social Science Quarterly*, 85(1), March, pp. 75-88.

[24] Thio, Alex. (2001). *Deviant Behavior*, 6th ed. Boston, Mass.: Allyn and Bacon.

[25] Wall, David S. (2007). "Policing Cybercrime: Situating the Public Police in Networks of Security within Cyberspace". *Police Practice and Research*, 8:2. Pp. 183-205. DOI 10.1080/15614260701377729.

[26] Wall, David S. & Matthew L. Williams. (2013). "Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing". *Policing and Society: Journal of Research and Policy*, 23:4, pp. 409-412. DOI 10.1080/10439463.2013.780222.

[27] Wells, Melissa. Et.al. (2007). "Defining Child Pornography: Law Enforcement Dilemmas in Investigations of Internet Child Pornography Possession". *Police Practice and Research: An International Journal*, 8:3, pp. 269-282. DOI 10.1080/15614260701450765.

[28] Williams, Katherine S. (2004). "Child Pornography Law: Does it Protect Children?". *Journal of Social Welfare and Family Law*, 26:3, pp. 245-261.

[29] Yar, Majid. (2009). *Cybercrime and Society*, London: Sage Publications Ltd.