

#### agus raharjo <agus.raharjo007@gmail.com>

## ICLJ 2017 : Please Activate Your Account

1 pesan

ICLJ 2017 <iclj@uinjkt.ac.id> Balas Ke: ICLJ 2017 <iclj@uinjkt.ac.id> Kepada: agus.raharjo007@gmail.com 5 Agustus 2017 pukul 17.16

Please do NOT reply this automail Always send your email to iclj@uinjkt.ac.id

Dear Prof. Agus Raharjo,

Your registration to ICLJ 2017 has been completed, please click the following link to activate your account:

http://iclj.event.uinjkt.ac.id/kfz/pages/activate.php?q=39&m=7427607938

Thank you. Best regards,

ICLJ 2017 Organizing Committee Homepage : http://iclj.event.uinjkt.ac.id/kfz Email : iclj@uinjkt.ac.id

Listed in Indonesia Conference Directory | http://ifory.net Automated Conference System provided by Konfrenzi | http://konfrenzi.com



## ICLJ 2017 : Your Account has been Activated

1 pesan

ICLJ 2017 <iclj@uinjkt.ac.id> Balas Ke: ICLJ 2017 <iclj@uinjkt.ac.id> Kepada: agus.raharjo007@gmail.com 6 Agustus 2017 pukul 23.58

Please do NOT reply this automail Always send your email to iclj@uinjkt.ac.id

Dear Prof. Agus Raharjo,

Your Account has been Activated.

User ID: USER-39 Please use this "User ID" in all correspondence (instead of your name).

Login Code: kz727769

You need the "Login Code" to login to our site, so please do not delete this email.

Please login to submit your abstract and paper.

Thank you. Best regards,

ICLJ 2017 Organizing Committee Homepage : http://iclj.event.uinjkt.ac.id/kfz Email : iclj@uinjkt.ac.id

Listed in Indonesia Conference Directory | http://ifory.net Automated Conference System provided by Konfrenzi | http://konfrenzi.com



## [ABS-6] Abstract Submitted to ICLJ 2017

3 pesan

ICLJ 2017 <iclj@uinjkt.ac.id> Balas Ke: ICLJ 2017 <iclj@uinjkt.ac.id> Kepada: agus.raharjo007@gmail.com 7 Agustus 2017 pukul 00.16

Please do NOT reply this automail Always send your email to iclj@uinjkt.ac.id

Dear Prof. Agus Raharjo,

We have received the submission of your abstract:

Abstract ID: ABS-6 Please use this "Abstract ID" in all correspondence (instead of abstract title).

Title:

CYBER CHILD PORNOGRAPHY: Law and Technology Problems in its Law Enforcement

Authors: Agus Raharjo

Institutions: Faculty of Law, Jenderal Soedirman University JI. Prof. dr. HR Boenyamin 708, Purwokerto 53122, Indonesia Email: agus.raharjo007@gmail.com

Content:

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

Topic: Universal vs Particular Values in Human Rights Practices

Presenter: Agus Raharjo

The Letter of Acceptance (LoA) can be downloaded from your account, once your abstract is accepted to be presented.

Thank you.

Best Regards, ICLJ 2017 Organizing Committee Website: http://iclj.event.uinjkt.ac.id/kfz Email: iclj@uinjkt.ac.id

#### Listed in Indonesia Conference Directory | http://ifory.net Automated Conference System provided by Konfrenzi | http://konfrenzi.com

**agus raharjo** <agus.raharjo007@gmail.com> Kepada: ICLJ 2017 <iclj@uinjkt.ac.id> 23 September 2017 pukul 11.02

Kok belum ada pengumuman hasil seleksi call for paper?

[Kutipan teks disembunyikan]

Internal Conference Law and Justice <iclj@uinjkt.ac.id> Kepada: agus raharjo <agus.raharjo007@gmail.com> 24 September 2017 pukul 21.45

Yang terhormat Bapak Agus Raharjo

Terimakasih atas emailnya. Saat ini panitia sedang menunggu hasil review abstrak dari TIM REVIEWER. Kami pastikan bahwa notifikasi diterimanya abstrak sesuai dengan jadwal yang telah ditentukan (25 September 2017).

Terimakasih

Panitia

ICLJ [Kutipan teks disembunyikan]



agus raharjo <agus.raharjo007@gmail.com>

## **Notification for Participants**

1 pesan

Internal Conference Law and Justice <iclj@uinjkt.ac.id> Kepada: agus raharjo <agus.raharjo007@gmail.com> 25 September 2017 pukul 13.31

Dear Prof. Agus Raharjo

Congratulation!

On behalf of the Academic Committee, we are delighted to inform you that on the strength of the paper submitted, your paper entitled "**CYBER CHILD PORNOGRAPHY: Law and Technology Problems in its Law Enforcement**" has been accepted for presentation at The 1st International Conference on Law and Justice (ICLJ 2017), November, 7-8, 2017, at Santika Hotel, BSD-City, South Tangerang, Indonesia.

The paper will be published in the Atlantis Conference Proceedings (Thomson Reuters Index). Please submit your full paper by October 21st, 2017, and pay the registration fee by October, 25th 2017. Please find the registration conference form will be attached in the next email.

Kind Regards

Asep Saepudin Jahar, Ph.D. The Conference Chairman



# KEMENTERIAN AGAMA UNIVERSITAS ISLAM NEGERI (UIN) SYARIF HIDAYATULLAH JAKARTA FAKULTAS SYARIAH DAN HUKUM

Jl. Ir. H. Juanda No. 95 Ciputat Tangerang Selatan

Telp. (021) 74711537 Website: www.uinjkt.ac.id, Email: humas<u>.fsh@uinjkt.ac.id</u>

Jakarta, 02 Oct 2017

NO : B-3402/FSH/HM.01.6/10/2017 Attachment : 1 File Subject : **Notification Participant** 

Dear

### Prof. Agus Raharjo

### Congratulation!

On behalf of the Academic Committee, we are delighted to inform you that on the strength of the paper submitted, your paper entitled **"Cyber Child Pornography: Law And Technology Problems In Its Law Enforcement"** has been accepted for presentation at The 1st International Conference on Law and Justice (ICLJ 2017), November, 7-8, 2017, at Santika Hotel, BSD-City, South Tangerang, Indonesia.

The paper will be published in the Atlantis Conference Proceedings (Thomson Reuters Index). Submit your full paper by October 21st, 2017, and pay the registration fee by October, 25th 2017. Please fill the registration conference form attached.

Kind Regards

The Conference Chairman



Asep Saepudin Jahar, Ph.D.

#### **Reviewer Comment:**

The topic of this paper is an important one. It places significant weight on the approach of Brenner which would not seem suitable when dealing with child pornography rather than cyber pornography in general, for example, 'strike back' & user self protection mechanisms. A more broadly based literature review would be helpful Perhaps also an examination of international measures such as specific legislation and definition, whether possession constitutes an offence, the role of ISPs in managing child cyber porn and the problems relating to child sexting.

# **CYBER CHILD PORNOGRAPHY**

Law and Technology Problems in its Law Enforcement

Agus Raharjo

Faculty of Law, 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 which keeps develop-ing, even when monetary crisis happened in this country. In the last two decades, pornography business was a business which got commercial success quickly. Unfortunately, the profit of this business cannot be obtained by each country. Only several countries that are able to gain the profit especially countries which have no strict regulation on morality. America is the state that mostly gains the profit from this business. It is the country which produces some hard-core films or videos more than 150 titles per week. America also receives the income from the sales of sex magazines, 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, the commercial value of this business cannot be known certainly.

If adult pornography matter in each country is different on behavior and regulation, in child porno-graphy matter, almost all countries have similarity which is prohibiting it. 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 causes the access to world wide web that provides 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 do self-improvement in dealing with the production and distribution of cyber child pornography. Beside Indo-nesia has included the country which operates the site with pornographic contents, Indonesia also includes 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 trying to create breakthrough in its investiga-tion process.

#### II. METHOD

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.

#### III. PREPARE YOUR PAPER BEFORE STYLING

#### A. The Regulation on Cyber Child Por-nography in Indonesia

The happening of sexual harassment cases toward children in 2016 triggers the government issue Government Regulation Substituting Law Number 17 Year 2016 which then becoming 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 spread 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).

This regulation does not give definition and specific regulation about child pornography. It only regulates the prohibition of child involvement in pornographic criminal act (Article 11) and child pro-tection from the influence and access to pornography (Article 15), as well as the imposition of obligation to government, social institutions, educational institutions, religious institutions, family, and/or society in founding, accompanying, and recovering social condi-tion, 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 regula-tion on this subject is found, 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 paragraph (1) actually 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 wide-ly 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 Telecommunica-tion 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 referring to the notion of pornography in general as it appears in pornography laws. The problem is not just the use or insertion of the word "child" in the legis-lation, but the material or criteria used may be dif-ferent. Because there is no definite definition, then the understanding of the legislation of other countries can be used as consideration in determining or defining cyber child pornography in the future.

A definition of the federal law in the United States as "a visual depiction of a minor engaged in sexually explicit conduct," has been causing harm to children for centuries (Magid, 2002). Other definitions can be cited from Canada. The Criminal Code now defines "child porn" as "a photographic, 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 depic-tion, for a sexual purpose, of a sexual organ or the anal region under the age of 18 years ... or any written mate-rial or visual representation that advocates or counsels sexual activity with a person under the age of 18 years ... "(Department of Justice Canada, 2002). Although there is no principal difference between these defini-tions and the general definition of pornography laws, the existence of strict regulations regarding cyber child pornography will have implications for law enforce-ment.

# B. 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 enforce-ment within the cybercrime prevention framework reacts in much the same way as traditional crime deals. 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 cri-mes 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 cri-mes. 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 combine to create an overload; law enforce-ment's ability to react to cybercrime erodes by cyber-crime and real-world crime in combination (Brenner, 2008).

This is the fact that causes cybercrime to 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 because 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 focusing attention and resources on crime occurring within their 'patch'. Yet, cybercrime, given the global nature of the Internet, is de-territorialized phenomenon. inherently Crimes in cyberspace bring together offenders, victims and targets that may well be physically situated in different countries and continents, and so the offenses spans national territories and boundaries (Yar, 2009).

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

Similarly, due process model, not suitable for complete cybercrime completely. The typology of due process model

with the negative model always empha-sizes 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 judi-cial power is in court, and it is said to be the final wall of justice, whereas cybercrime cannot be quickly pre-vented 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. Techno-logy – in the form of computer, personal digital assis-tants, 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 technocomponent of life transform our environment in the twentyfirst 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 is smash the boundaries, tear down the hierarchy and dismantle the bureaucracy (Lipnack and Stamps, 1994). Networks, unlike hierarchies, are lateral, fluid systems. Networks, unlike hierarchies, decentralize power and authority, 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. The issue for Indo-nesia is whether the state budget is sufficient to finance the addition of police personnel. It's a classic problem that always hit the police when faced with a relatively new crime. Second, the formations of cyber police or cyber cop, which specifically deal with cybercrime problems and can quickly, reacted if there is an inci-dent. 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 "pat-rol" 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).

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 ad 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 inforporate 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. Clearly, 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 correct proportion, for example, as an ultimum remidium, by promoting public participation (Internet users) in crime prevention.

Another model introduced by Brenner is pre-vention 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 complete 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 guarantee 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 func-tions 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 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 regula-tion 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 pornogra-phy should keep developing 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 techni-cal 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..." Those efforts need to be followed by activities to catch and process pedophiles legally. There must be a cooperation done by law enforcer and people to rescue the next generation from early sexual exploitation.

#### IV. CONCLUTION

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 partici-pation from the people for law enforcement, and no development of software to prevent on an ongoing ba-sis. 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 porno-graphy; third, there needs to be improvement on tech-nical 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.

#### ACKNOWLEDGMENT

The researcher would like to express gratitude to some of the parties who has helped researcher during looking for data and finishing this paper. First and foremost, the researcher express 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 Wahyuni, and Enamel Audha, which has been helpful in searching data. Hopefully the help given to receive a reply from Allah SWT.

•

#### REFERENCES

- BBC News (2001, August 8). U.S. breaks child cyber-porn ring. Retrieved March 11, 2006, from <u>http://news.bbc.co.uk/1/hi/world/americas/1481253.stm</u>, access on 27<sup>th</sup> May 2014.
- [2] Brenner, Susan W. (2004). Toward a Criminal Law for Cyberspace: Distributed Security". 10 Boston University Journal of Science & Technology Law 1.
- [3] 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
- [4] 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
- [5] 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 <u>http://canada.justice.gc.ca/en/news/nr/2002/</u> <u>doc 30531.html</u>, access on August 24<sup>th</sup> 2010.

- [6] Fisher, William, and Azy Barak. (2000). "Online Sex Shops: Phenomenological, and Ideological Perspectives on Internet Sexuality." Cyber Psychology & Behavior 3:575–89.
- [7] Lipnack, Jessica & Jeffrey Stamps. (1994). The Age of the Network, Organizing Principles for the 21<sup>st</sup> Century, New York: John Wiley & Sons.
- [8] Magid, L. (2002, March 21). Net users can help fight child porn. Retrieved March 9, 2006, from <u>http://www.pcanswer.com/articles/sjm\_childporn.htm</u>, access on 15<sup>th</sup> June 2014.
- [9] McQuede III, Samuel C. (ed). (2009). Encylopedia of Cybercrime. Westport CT: Greenwood Press.
- [10] Putnam, D. E. (2000). "Initiation and Maintenance of Online Sexual Compulsivity. Implications for Assessment and Treatment", *Cyber Psychology and Behavior* 3, pp. 553–64.
- [11] Raharjo, Agus. (2013, June). Pencegahan Cybercrime Melalui Pengembangan Prinsip Pertanggungjawaban Pidana Bagi Pengguna Internet, Paper on Seminar Nasional Hukum Pidana, Purwokerto.
- [12] 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
- [13] 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.
- [14] Thio, Alex. (2001). *Deviant Behavior*, 6th ed. Boston, Mass.: Allyn and Bacon
- [15] Yar, Majid. (2009). *Cybercrime and Society*, London: Sage Publications Ltd.

# The 1<sup>st</sup> International Conference on Law and Justice (ICLJ) November 7 – 8, 2017

Faculty of Sharia and Law, Islamic State University Jakarta (UIN JAKARTA) Hotel Santika, BSD-City, South Tangerang, Banten, INDONESIA

## Date: November, 7-8, 2017 Venue: Santika Hotel, BSD-City, South Tangerang, Banten, Indonesia

# **Conference Registration Form**

All participants are required to complete this registration form and return in MS Word format to ICLJ Committee (email to iclj@uinjkt.ac.id )

## SECTION 1: CONTACT INFORMATION

| TITLE:                              | Mr Mrs                    | □Ms □Dr 凶P  | rof. 🗌 Other, specify:         |                           |  |
|-------------------------------------|---------------------------|---|--------------------------------|---------------------------|--|
| FIRST NAME:                         | Agus                      |   | LAST NAME:                     | Raharjo                   |  |
| ADDRESS:                            | Faculty of Law, Jende     | eral Soedirman University                           | MAIN TELEPHONE:                | 0281 638339               |  |
|                                     |                           | l. Prof. dr. HR. Boenyamin<br>Kec. Purwokerto Utara | WORK TELEPHONE (if different)  | 0281 638339               |  |
|                                     | , to, non or endeng, r    |   | HOME TELEPHONE                 | 0281 633246               |  |
| TOWN/CITY:                          | Banyumas                  | MOBILE PHONE: +62 81327226556                       |                                |                           |  |
| POST CODE;                          | 53122                     |   | PRIMARY EMAIL:                 | agus.raharjo007@gmail.com |  |
| COUNTRY;                            | Indonesia                 |   | SECONDARY EMAIL:               | agus.raharjo999@gmail.com |  |
| FACULTY/DEPART                      | MENT/SCHOOL:              | Law/Criminal Law                                    |                                |                           |  |
| AFFILIATION (NAM<br>UNIVERSITY/INST |                           | Jenderal Soedirman University                       |                                |                           |  |
| FIELD OF RESEARC                    | <del>.H</del>             | Cybercrime  |                                |                           |  |
| Are you willing to                  | serve as a session chair: | □Yes ☑No  |                                | Malandar (1997)           |  |
| How did you hea<br>conference?      | r about this              | □Direct Email                                       | Vebsites (Please Specify)<br>: |                           |  |

#### **SECTION 2: PAPER PRESENTATION**

| Are you presenting a paper or as a participant? | Presenting Paper | If you are presenting a paper, how many are you 1 2 presenting? |  |
|---|------------------|---|--|
|---|------------------|---|--|

#### **SECTION 3: PAYMENT INFORMATION**

I'll send my registration fee USD(\$200)/IDR(Rp.2.000.000) \_\_\_\_\_ (amount) via bank transfer.

Please note that transfer fees charged by the bank must be covered by the participants themselves.

| SIGNED:<br>(or write name here) |   | DATE: 21 That 2017 | / |
|---------------------------------|---|--------------------|---|
|                                 | V |                    |   |



agus raharjo <agus.raharjo007@gmail.com>

## **Conference Schedule**

2 pesan

Internal Conference Law and Justice <icij@uinjkt.ac.id> 5 November 2017 pukul 19.41 Kepada: agus raharjo <agus.raharjo007@gmail.com>, Yayan Sopyan <yayan\_sopyan@uinjkt.ac.id>, mujar syarif <mujarsyarif@yahoo.com>, Lushiana Primasari <lushiana\_hukumuns@yahoo.com>, "Dr. Saadiya Asstt. Professor (F/o Law)" <saadiya@jmi.ac.in>, fidiyani.rini@gmail.com, Khamami Zada <khamamizada@gmail.com>, Natasya Fila Rais <natasya.filarais@gmail.com>, qurrataayuni <qurrataayuni@ui.ac.id>, Euis Amalia <euis.amalia@uinjkt.ac.id>, Yuke Rahmawati <yuke.rahmawati@uinjkt.ac.id>, Dewi Sukarti <dewi.sukarti@uinjkt.ac.id>, Asmawi UIN Jakarta <asmawi@uinjkt.ac.id>, Nur Hayati <maf\_lubis74@yahoo.com>, mashudi\_69@yahoo.co.id, Muhammad Ishar Helmi <izharhelmi@uinjkt.ac.id>, Saru Arifin <saruarifin@mail.unnes.ac.id>, Hidayatulloh Asmawih <hidayatulloh87@uinjkt.ac.id>

Dear

## Presenter

On behalf of the Academic Committee, we are delighted to inform you that on the strength of the paper submitted, has been scheduled for presentation at The 1st International Conference on Law and Justice (ICLJ 2017), November, 7-8, 2017, at Santika Hotel, BSD-City, South Tangerang, Indonesia. Kindly find the email attachment.

Kind Regards,

ICLJ Committee.

Gmail - Conference Schedule



#### Yuke Rahmawati <yuke.rahmawati@uinjkt.ac.id>

6 November 2017 pukul 09.35

Kepada: Internal Conference Law and Justice <iclj@uinjkt.ac.id>

Cc: agus raharjo <agus.raharjo007@gmail.com>, Yayan Sopyan <yayan\_sopyan@uinjkt.ac.id>, mujar syarif <mujarsyarif@yahoo.com>, Lushiana Primasari <lushiana\_hukumuns@yahoo.com>, "Dr. Saadiya Asstt. Professor (F/o Law)" <saadiya@jmi.ac.in>, fidiyani.rini@gmail.com, Khamami Zada <khamamizada@gmail.com>, Natasya Fila Rais <natasya.filarais@gmail.com>, qurrataayuni <qurrataayuni@ui.ac.id>, Euis Amalia <euis.amalia@uinjkt.ac.id>, Dewi Sukarti <dewi.sukarti@uinjkt.ac.id>, Asmawi UIN Jakarta <asmawi@uinjkt.ac.id>, Nur Hayati

<maf\_lubis74@yahoo.com>, mashudi\_69@yahoo.co.id, Muhammad Ishar Helmi <izharhelmi@uinjkt.ac.id>, Saru Arifin <saruarifin@mail.unnes.ac.id>, Hidayatulloh Asmawih <hidayatulloh87@uinjkt.ac.id>

Received, thank you. [Kutipan teks disembunyikan]

## The 1<sup>st</sup> International Conference on Law and Justice (ICLJ) November 7 – 8, 2017 Faculty of Sharia and Law, Islamic State University Jakarta (UIN JAKARTA) Hotel Santika, BSD-City, South Tangerang, Banten, INDONESIA

# ICLJ CONFERENCE SCHEDULE

| DATE/TIME                   | ACTIVITY/SESSION  | PERSON  | PLACE | PIC |
|-----------------------------|---|---|-------|-----|
| Nov, 7 <sup>th</sup> , 2017 | DAYI  |   |       |     |
| 07.00-08.00 AM              | Registration  | Committee   |       |     |
| 08.05-09.45 AM              | Opening Ceremony  |   |       |     |
| 09.45-10.00 AM              | BREAK   |   |       |     |
| 10.00-12.30 PM              | Plenary Session I:<br>Human Rights, Theory<br>and Practices | <ul> <li>Invited Speakers <ol> <li>Prof. Dr. Tim Lindsey <ul> <li>Justice for All and anti-Discrimination</li> </ul> </li> <li>Prof. Dr. Masykuri Abdillah <ul> <li>Islam and Human Rights: Theoretical and Practical Framework in <ul> <li>Indonesia</li> </ul> </li> <li>Prof. Dr. Razeen Sappideen <ul> <li>Universal vs Particular Values in Human Rights Practices</li> </ul> </li> <li>Dr. Ved Pal Singh Deswal. <ul> <li>Alternative Dispute Resolution as a tool of Speedy Justice: Glimpses <ul> <li>from India</li> </ul> </li> </ul> </li> </ul></li></ol></li></ul> | MAIN  |     |
| 12.30-01.30 PM              | BREAK   |   |       |     |
| 01.30-03.30 PM              | Panel Discussion I:   |   |       |     |

| DATE/TIME      | ACTIVITY/SESSION                             | PERSON  | PLACE | PIC |
|----------------|--|---|-------|-----|
| 01.30-03.30 PM | Business, Human Rights<br>and Accountability | <ul> <li>Chairman:<br/>Arie Afriansyah, SH, MIL, Ph.D<br/>Business, Human Rights and Accountability</li> <li>Presenter: <ol> <li>Indra Rahmatullah<br/>The Concept Of Human Rights Due Diligence Toward The<br/>Corporation Of Fishery Sector In Indonesia</li> <li>Jalaluddin Al-Banjary<br/>Coal Mining And Human Rights (Initiating The Right To A Good And<br/>Healthy Environment As Non Derogable Right)</li> <li>Dr. Helza Nova Lita,SH, MH. Prof. Eman Suparman SH,MH. Dr.<br/>Renny Supriatni,SH,MH. Dr. Dadang Epi, SH,MH<br/>Application of Customary Law in Improving Economic Welfare of<br/>Adat Village Community (Case study of economic potential of Adat<br/>Village in West Java)</li> </ol></li></ul> | A     |     |

| DATE/TIME      | ACTIVITY/SESSION   | PERSON   | PLACE | PIC |
|----------------|--|--|-------|-----|
| 01.30-03.30 PM | Universal vs Particular<br>Values in Human Rights:<br>Women and Family Law | <ul> <li>Chairman: <ol> <li>Dr. Suaidi Asyari, MA, Ph.D<br/>Strengthening Islamic Institution for The Shake of Religious<br/>Minority rights</li> </ol> </li> <li>Presenter: <ol> <li>Mutiara Hikmah Subiyakto and Eva Achjani Zulfa<br/>Abortion in Indonesia From The Womwn"s Rights and Islamic Law<br/>Perspectives</li> <li>Yayan Sopyan and Burhanatut Dyana<br/>The Legality Of Marriage For Indonesia Migrant Workers (Seeking<br/>The Effort Of Indonesia Government In Certainty Of Law For<br/>Indonesia Migrant Workers In Tawau, Sabah, Malaysia)</li> <li>Prof. Dr. Agus Raharjo<br/>Cyber Child Pornography: Law And Technology Problems In Its Law<br/>Enforcement</li> <li>Dr. Saadiya<br/>Muslim Personal Law and Gender Equality Concerns in India</li> <li>Ardi Natakusuma Sanjaya, Okti Putri Andini, and Rizky Noor<br/>Fajrina<br/>Equality of Human Right for Sales Promotion Girls</li> </ol></li></ul> | В     |     |

| DATE/TIME      | ACTIVITY/SESSION                            | PERSON   | PLACE | PIC |
|----------------|---|--|-------|-----|
| 01.30-03.30 PM | Justice for All and Anti-<br>discrimination | <ul> <li>Chairman: <ol> <li>Cristoph Sutter (ICRC) </li> <li>Justice for All and Anti-discrimination</li> </ol> </li> <li>Dr. Mhd. Ibrahim Khalil Bhuiyan </li> <li>Bresenters: <ol> <li>Natasya Fila Rais </li> <li>The Implementation Of Sustainable Development Goals To Stop Marital Rape In Indonesia</li> <li>Saifudin Asrori </li> <li>Institutional Religious Dialogue; Strengthening Cooperation And Harmony Between Religious Communities In Indonesia</li> </ol> </li> <li>Shinta Dewi Rismawati </li> <li>Quo Vadis Women In Islamic Political Parties (A Study Of Legal Culture Of Women Legislative Candidates Recruiting In Elections In Pekalongan Indonesia)</li> <li>Rini Fidiyani </li> <li>State Legal Protection On Freedom Of Religion: A Myth</li> <li>Dr. Khamami Zada </li> <li>Collaborative Protection Of Moslem Rohingya Seekers In North Aceh</li> <li>Qurrata Ayuni SH MCDR </li> <li>Judicial Review of Criminal Code Articles on Adultery, Rape and Same-sex Obscene in the Constitutional Court </li> <li>Budi Juliandi /Saifuddin Herlambang </li> <li> <i>"Unit Compute State Compute State Compute State Compute State Computer State Computer State Computer State Computer State Constitutional Court  </i></li> </ul> | C     |     |

| DATE/TIME                   | ACTIVITY/SESSION | PERSON   | PLACE | PIC |
|-----------------------------|------------------|--|-------|-----|
| Nov, 8 <sup>th</sup> , 2017 | Day II           |  |       |     |
| 07.00-08.00 AM              | Registration     | Committee  |       |     |
|                             | Registration     | Committee         Invited Speakers:         1. Prof. Dr. Nik Kamal         Good Governance Human Rights and Social Welfare         2. Prof. Dr. M. Arskal Salim, GP, M.Ag         Good Governance in Strengthening Islamic Institution         3. Prof. Ruhaini Dzuhayatin         Good Governance and Gender Mainstreaming         4. Dr. Asep Saefuddin Jahar, MA         Public Policy and Strategies for Promoting Socio-Economic Justice         Moderator: Nur Hidayah, Ph.D | MAIN  |     |
|                             |                  |  |       |     |
| 10.00-11.00 AM              | BRAKE            |  |       |     |

| DATE/TIME      | ACTIVITY/SESSION   | PERSON  | PLACE | PIC |
|----------------|--|---|-------|-----|
| 11.00-01.00 PM | Panel Discussion II<br>Islam and Good<br>Governance          |   |       |     |
| 11.00-01.00 PM | The Sharia and Its Role<br>in Economic and Social<br>Justice | <ul> <li>Chairman: <ol> <li>Ir. Muh. Nadratuzzaman, MS, MSc., Ph.D<br/>Analysis of Corporate Governance in Shariah Banks in Indonesia</li> <li>Alfitri, M.Ag, LLM, Ph.D<br/>Sharia, Legal Fiction, and Popular Supports: Compliance with<br/>Corporate Zakat Duty in Indonesian Islamic Commercial Banks</li> </ol> </li> <li>Presenters: <ol> <li>Euis Amalia and Nurhidayah<br/>Zakat for Socio-Economic Justice in Indonesia: Critics of Policies and<br/>Framework for Good Corporate Governance</li> <li>Muhammad Nadratuzzaman Hosen and Nasimul Falah **<br/>Analysis of Corporate Governance in Shariah Banks in Indonesia</li> <li>Nun Harrieti S.H., M.H.<br/>Dr Etty Mulyati, S.H., M.H.<br/>Concept Of Waqf Bank On Islamic Banking Law Perspective In<br/>Indonesia</li> <li>Dewi Sukarti Isnawati Rais<br/>Islamic Inheritance Law For Economic Social Justice In Indonesia</li> <li>Yuke Rahmawati<br/>BMT Accounting in Perspective Compilation of Islamic Economic<br/>Law (KHES)</li> </ol> </li> </ul> | D     |     |

| DATE/TIME      | ACTIVITY/SESSION   | PERSON   | PLACE | PIC |
|----------------|--|--|-------|-----|
| 11.00-01.00 PM | Good Governance in<br>Strengthening Islamic<br>Institution | <ul> <li>Chairman: <ol> <li>Dr. JM. Muslimin<br/>Good Governance in Strengthening Islamic Institution<br/>Presenters:</li> <li>Natasya Fila Rais<br/>Application Of Democracy In Indonesia And How It Guarantees<br/>Muslim Women's Freedom Of Living</li> <li>Jeanne Francoise<br/>Good Governance and Human Rights Based on the Thoughts of<br/>Syeikh Muhammad Abduh: Indonesian Perspective</li> <li>Dr. Nurhayati, M.Ag and Dr. Jailani, M.Ag<br/>The Implementation Of Criminal Act Of Adultery (Comparative<br/>Study Between Islamic Jurisprudence Of Legal School And Qanun<br/>Jinayat In Aceh )</li> <li>Asni<br/>The Existence Of Islamic Legal Institutions In Realizing Social Justice<br/>In The Buton Sultanate</li> <li>Dr. Muamar Hasan Salameh<br/>The principle of the separation of powers between sharia and the<br/>statutory law</li> <li>Dr.Lutfullah Saqib<br/>A Realistic Approach to the Concept of Mediation and its possible<br/>Role in Social and Institutional Justice in Pakistan (A Comparative<br/>Study of Sharī'ah and Law)</li> </ol></li></ul> | E     |     |
| 01.00-02.00 PM | BREAK  |  |       |     |

| DATE/TIME      | ACTIVITY/SESSION                       | PERSON  | PLACE | PIC |
|----------------|--|---|-------|-----|
| 02.00-04.00 PM | Panel Session III                      |   |       |     |
| 02.00-04.00 PM | Good Governance and<br>State Mechanism | <ul> <li>Chairman: <ol> <li>Prof. Dr. Carolyn Sappiden<br/>Good Governance and State Mechanism</li> <li>Zainal Abidin, SH, MA PhD (UGM Yk)</li> </ol> </li> <li>Pemakalah <ol> <li>Titut Amalia<br/>Corruption Prevention Through Participative Process Of<br/>Development Planning</li> <li>Osuagwu Ugochukwu Esq<br/>Women And Democratic Governance In Nigeria</li> <li>Muhammad Ishar Helmi<br/>Structuring Authority Of The KPK As An Anti-Corruption Agency</li> <li>Mashudi<br/>Social Sanction Versus Legal Sanction In Corruption Case</li> <li>Nimish Arjaria<br/>Democracy And Good Governance.</li> </ol> </li> </ul> | F     |     |

| DATE/TIME      | ACTIVITY/SESSION   | PERSON  | PLACE | PIC |
|----------------|--|---|-------|-----|
| 02.00-04.00 PM | Public Policy and<br>Strategies for Promoting<br>Socio-Economic Justice:<br>Protecting Public Interest | <ul> <li>Chairman:</li> <li>Heru Sesetyo, SH, LLM, PhD<br/>Public Policy and Strategies for Promoting Socio-Economic Justice</li> <li>Dr. Pheni Chalid<br/>Public Policy and Strategies for Promoting Socio-Economic Justice</li> <li>Dr. Yetty Komalasari, SH, LLM<br/>Institutional Aspect of Good Governance: Protection Public Interest</li> <li>Presenters:</li> <li>Dr. Babak Pourghahramani<br/>An Elaboration on Computer Frauds from the Perspective of Irans<br/>Law and International Instruments</li> <li>Hazar Kusmayanti; Linda Rachmainy; Sherly Ayuna Putri<br/>Mobile Court Practice and Realization of Indonesia Civil Law<br/>Principles: A Case Study of West Java Islamic Court</li> <li>Eka Nugraha Putra<br/>E-Commerce Certificate Authority Implementation to Protecting<br/>Consumer Rights</li> <li>Hidayatulloh<br/>Protecting Public Interest From Price Fixing Cartel: The Case Of<br/>Honda And Yamaha In Indonesia</li> </ul> | G     |     |

| DATE/TIME      | ACTIVITY/SESSION | PERSON    | PLACE | PIC |
|----------------|------------------|-----------|-------|-----|
| 02.00-04.00 PM | Academic Forum   | Dean Form | Н     |     |
|                |                  |           |       |     |
| 04.00 PM       | Closing Ceremony | Committee | MAIN  |     |