THE ROLE OF INTERNATIONAL COOPERATION IN PREVENTING AND OVERCOMING CYBERCRIME, IN PARTICULAR CYBERPORNOGRAPHY

By Dr I.B.R Supancana[1]

[1]Chairman/Founder of Indoregulation, Centre for Regulatory Research.

I. INTRODUCTION

For the purpose of conducting a comprehensive study and analysis on the role of international cooperation in preventing and overcoming cybercrime, including cyber pornography, first of all it is important to have some background information in the form of facts and data concerning the recent development of cybercrime both at the international and national level. In addition, there is a need to formulate the scope of cyber crime that requires further attention in the context of promoting international cooperation. Further clarification is also required to certain aspects related to cyber pornography, such as: its definition and meaning; the distinction between pornography and cyber pornography; and the challenges that we have to encounter.

A. Facts and Data concerning the development of cyber crime:

1. An IT Company so called Computer Associate (CA), has mapped the existence of seven (7) attack patterns that potentially threat internet in 2007 with increasing intensity. At least there are a number of attack pattern that would threat internet. The attacks are deemed more sophisticated in stealing Intellectual Property Rights (IPR), personal identity, content and cross border financial report, both to organization and social network. There are many malware that could destroy network such as Trojan, worm, virus and spyware. Phiser has shown their improving capabilities with social engineering tactics. Spamming also showing increasing trend by utilizing "spam image based" which could break all anti spam filter. The cheap cost of disseminating spam through botnet could be used by cyber criminals to disseminate Trojan. Meanwhile local made computer virus such as "pacaran" has spread by relying on format to attack the data at local computer network[2].

2. The US Federal Trade Commission notes consumer report against 670.000 frauds (fraud and identity theft) in the year of 2006 with the loss of about US$ 1,2 billion. Identity theft was in the first place with the percentage of 36% or equal to 2,466,035. Other form of identity theft is credit card fraud (carding) with about 25%, followed by phone or utility fraud and bank fraud. Identity theft is followed by other form of theft, such as Shop at Home, catalogue fraud: fraud in prices, sweep stakes and lottery, fraud at internet auction web sites or fraud at internet auction web sites[3].

3. Mid year report of the Internet Security Threat Report (from software vendor Symantec) stating that about 157.000 unique phising messages were sent all over the world during the first mid year of 2006, a growth of about 81% compared to the same period in 2005[4].

4. AT & T reported that as the consequences of hacking which illegally access to computer information and stole credit card information and personal data of thousands of consumers who bought DSL equipment from AT &T's online store. Personal data of almost 19.000 consumers were attacked by hackers. On other occasion,

[2]See Roni Yunianto: "CA: Serangan ke Inernet makin canggih", Bisnis Indonesia, 13 February 2007.

[3]Christopher S Rugaber, "Identity Theft tops consumer complaints in 2006: FTC Report", The Jakarta Post, 9 February 2007.

[4] Reuters, "Criminal flock to the internet , survey finds", 23 September 2006.

an NGO called Privacy Rights Clearing House counted more than 170 violations of internet security consumers by openly disclose such sensitive personal information[5].

The above data and facts have shown significant increase of cybercrime, both in terms of quantity, quality, frequency and its modus operandi. The above mentioned facts create concern among stakeholders that cyber crime could attack anybody, both individual, consumers, corporations, governments, and other legal entity in unexpected ways and modus operandi, with possible fatal results (consequences). Meanwhile the scope of activities of cybercriminals can not be confined to territorial borders and jurisdictions, which add to its complication in the efforts to uncover, prosecute, hear and decide the case through court proceedings, including its law enforcement. In order to prevent, minimise and overcome cybercrime it requires international and across sectoral cooperation, and involving private-public partnership and participation from all components of society.

B. The Scope of Cybercrime

The previous analysis on cybercrime provides us with some pictures concerning the broad spectrum of cybercrime and the scope of cybercrime that may cover different field of activities, among others:

1. Broadcasting

   Some acts of crime relevant to broadcasting may include: mockering, humiliating, slandering, defamation, mislead, lie, incite, insulting, violence, neglecting religious value, human dignity, and jeopardizing international relations.

2. Ethics

   Variable of crimes related to ethics are, among others: paedophilia, sexual exploitation of children, live sex shows, obscene and indecent transmission, obscene and indecent telephone calls.

3. Telematic

   Hacking, cracking, illegal interception, data interference, system interference, abuse of equipment, forgery related to computer, fraud by using computer.

4. Intellectual Property Rights

   Intellectual property rights' infringement can be in the form of: copyrights infringement, cybersquating, cyberparasites, typosquating,, domain hijacking.

[5]Associated Press "Hackers took credit card customer info, says AT & T", as aquote by The Jakarta Post, 31 August 2006.

5. Taxation

   Tax evasion and tax embezzlement of taxable transaction via internet are some of its examples.

6. Privacy

   Identity theft; illegal access and dissemination of privacy and sensitive personal data are some of the examples.

7. Trade and Finance

   Spamming, internet scam, carding, page jacking, phising, security fraud, cyberlaundering, illegal trafficking of alcohol and drug are types of cybercrime in the field of trade and finance.

8. Terrorism

9. Etc.

C. Cyberpornography as a part of Cybercrime

1. Definition

   Originally coming from Greek word "Porno, meaning prostitutes and graphos, meaning writing... (it) include (s) the depiction of actual sexual content... and depiction of...nudity or lascivious exhibition".

2. Pornography on the Internet

   These ranges from pictures, short animation movie, sound files or stories (via both web and usenet). It also possible to see live sex shows by connecting to some World Wide Web... sites by using special software (downloadable).

3. Some characteristics of Cyberpornography compare to other Pornography

   - it can be infinitely copied and distributed at minimal cost
   - the quality of image does not degrade on copying
   - it is difficult for law enforcement to detect due to the size and structure of the internet and the availability of encryption.

4. Some Challenges on the Issue of Cyberpornography, particularly Childpornography[6]:

   - We take steps to ensure that we can obtain evidence necessary to identify child pornographers;
   - We must respect the right to privacy and laws protecting it and use proper legal process to obtain data, but we must also make sure

[6]Views expressed by Eric Holder, Deputy Attorney General of the US before International Conference "Combating Child Pornography on the Internet", Vienna, Austria, 29 September 1999.

that such laws are not so strict that effective enforcement is not possible;

- We must work together, hot lines, law enforcer and private industry;
- We must work together to educate our citizens and consumers about tools and other resources to filter and protect children from harmful content.

II. Characteristics of Cybercrime, Its Regulatory Challenges and Law Enforcement

A. Characteristics of Cybercrime

1. Transnational

Computer related crime are international in nature, and that important public safety issues must be considered as we work to harness the internet's power to communicate, engage in commerce and expand people's educations opportunities across the globe. Our Success in securing our network depends on our ability to develop a coordinated response to criminal activities on our computer system[7].

The characteristics of transnational crime are:

- It is committed in more than one State;
- It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State;
- It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State;
- It is committed in one State but has substantial effects in another State[8].

2. Anonymity

In cyberworld, it is possible and easy for a person to remain "anonymous" by hiding its identity while keep an on-line communication. This become possible since such communication is more in the form of "bytes" and "text" rather than pictures or voices. The physical address from where someone interacts may not be easy to be identified. So anybody can access the computer through joint computers or public computer, communicating with anybody without necessity to disclose their identity. Though somebody can be traced via user internet protocol (IP) address of the computer that

[7]Kevin Di Gregory, "Fighting Cybercrime- what are the Challenges Facing Europe", Remarks at meeting before The European Parliament, 19 September 2000.

[8]Article 3.2 of the UN Convention against Transnational Organized Crime of 2000 which entry into force on 29 of September 2003.

they use, but it is difficult to identify it in situation where such equipment is not connected to somebody or to identifiable legal entity[9]. In the context of efforts to prevent and curb cybercrime, such anonymity will finally lead to creating technical constraints to trace cybercriminals.

B. Regulatory Challenges and its Law Enforcement

1. Jurisdictional Issues

The jurisdictional issues are complicated issues in revealing, preventing and overcoming cybercriminals as there are connected to different concepts of jurisdiction, such as: power to legislate; power to hear and adjudicate; subject matter jurisdiction; personal jurisdiction; forum convenience; forum non-convenience; governing law or choice of law; and enforcement of judgements.

The jurisdictional issues may become more complex in the situation where more than one States Claim to have jurisdiction to hear and adjudicate cases on cybercrime based on different considerations and interests. In such situation, in order to determine which jurisdiction shall apply there are certain parameters than can be used, among others: personal jurisdiction; subject matter jurisdiction; jurisdiction based on venue; and jurisdiction based on enforcement of the judgements[10].

On personal jurisdiction, the court can not validly act if it does not have personal jurisdictions over the parties of the suit. This is based on recognition of certain limitations of any court's power to compel defendants to appear and defend themselves.

On subject matter jurisdiction, courts are restricted in terms of the kind of disputes they can adjudicate. It is necessary for a court to act in valid manners, courts that do not have subject matter jurisdiction over the particular disputes brought to it must dismiss such claims when they are presented before it.

Venue rules are designed to protect defendants against being sued in "inconvenient" places. Venue rules are not "fundamental" in the same way that rules regarding personal jurisdiction and subject matter jurisdiction.

On Choice of Law, in case the parties have determined choice of law, such choice of law shall apply. In case no choice of law exists, choice of law can be based on: the domicile of the plaintiff; defendant; where

[9]See Sonny Zulhuda, "Copyright Law in the Cyberspace", unpublished, page 2.

[10]See Yee Fen Lim, Cyberspace Law: Commentaries and Materials, Oxford University Press, 2003 (reprinted edition), page 19-20.

the court sits; the transaction; etc.

Enforcement of the judgments is another important issue relevant to jurisdiction as there is a need to get support for enforcement of the judgement. This may be a complex undertaking if, for example the defendant and his asset are physically located within the boundaries of other jurisdictions.

The abovementioned jurisdictional issues can not be settled if there is no good relations both among States through legal cooperation, extradition treaty, mutual legal assistance in criminal matters etc which will further be elaborated.

2. The Issue of Identifying Cybercriminals

Another thorny issue stem from the lack of identification mechanisms on global networks, and the fact that individuals can be anonymous or take on masked identities (i.e., adopt false personas by providing inaccurate biographical information and misleading screen names)[11].

The difficulties in locating and identifying cybercriminals are caused by[12]:

a. Divested and diverse environment

b. Wireless and satellite communication

c. Difficulties in conducting real time tracing

d. Technical infrastructure and data retention

e. Anonymity of internet communication

3. The Issue of Taking Evidence

The progress in computer science and technology enable a computer to store a tremendous amount of information, including evidence that might not be known to the computer's owner. This feature of computer information can present law enforcement challenges by highlighting the need for training and expertise (and time) for the information to be recovered. The difficulty of the search and recovery of information may depend on how familiar the forensic expert is with the particular hardware and software configuration of the computer at issue.

4. The Issue of Infrastructure Protection

Protecting information infrastructure is imperative but difficult for a host of reasons: the number of different systems involved, the interdependency of these systems, the various nature of the threats (physical and cyber, military, intelligence, criminal,

[11]See Yee Fen Lim, Ibid, page 258.
[12]Ibid, page 265-268.

natural), and the fact that many of these infrastructure are maintained primarily by the commercial sectors[13].

III. International Cooperation in Preventing and Overcoming Cybercrime

A. Harmonising National Law with Relevant International Legal Instruments

1. International Legal Instruments

In the efforts to prevent and overcome cybercrime, particularly in promoting international cooperation, there are some international legal instruments, both hard laws and soft laws that could be considered. There are several international legal instruments that contain provisions on international cooperation relevant to preventing and combating cybercrime. It covers, among others:

a. Council of Europe Convention on Cybercrime of 2001

By considering the transnational character of computer, the steps to prevent and combat cybercrime shall be complemented with international cooperation. For that reason this Convention requiring the State parties, on mutual basis, to provide certain form of assistance, for example by maintaining and taking care of evidence and by localising cybercriminals. The Convention also accommodates international cooperation in the form of transborder computer search. The forms of traditional mutual legal assistance and extradition can also be accommodated by this agreement. A framework that operates 24 hours a day and 7 (seven) days a week and "national contact point" to be established mayspeed-upinternational investigations against cybercrime[14].

The convention has rightly formulates provisions on general principles of international cooperation in the following sentence:

"The parties shall cooperate with each other.....to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection

[13]Ibid, page 260.

[14]See Abubakar Munir, "Cyberterrorism: The National and International Legal Initiatives", unpublished, page 7.

of evidence in electronic form of criminal offence[15].

The above international cooperation covers quite wide scope of information, include not only investigation or proceedings against crime relevant to computer system and data, but also covering the use of electronic form of evidence[16].

b. Organization of Economic Cooperation and Development (OECD) Framework

Within the framework of OECD there are several documents relevant to international cooperation, namely:

- Guidelines for the Security of Information System and Networks toward a Culture of Society, 7 August 2002;
- OECD-APEC Global Forum: Policy Framework for the Digital Economy, 15 January 2003;
- OECD Guidelines for Cryptography Policy, 1996.

c. G-8 Framework

Within the framework of G-8 (USA, Canada, French, Germany, Italy, Japan, Russia and UK) there are several documents and important initiatives relevant to international cooperation in preventing and combating cybercrime, among others:

- Principles and Action Plan to Combat Computer Related Crime of 1998. It consists of 10 principles and action plan as an effort to identify cybercriminals on the internet and to trace responsible parties who conduct crime through the internet;
- G-8 Sub Group on High Tech Crime jointly with EU Commissioner on 10-14 May of 2004 discussing 4 main topics , including on combating cybercrime and enhancing cyber investigation[17];
- G-8 24/7 Networks which oblige its 20 State parties to establish point of

[15]Article 23 of Budapest Convention on Cybercrime of 2001.
[16]See also, Statement of Bruce Swartz, Deputy Assistant Attorney General before Senate Foreign Relation Committee concerning "Multilateral Law Enforcement Treaties", 13 July 2004.

[17]Other issues that were discussed include: Prevention of Terrorism and Serious Criminal Act; Border and Transportation Security; Fighting Foreign Official Corruption and Recovering Stolen National Asset. For further detail, see http/www.cybercrime.gov.htm.

contact that works 24 hours a day and 7 days a week to provide investigational assistance against cybercrime[18].

d. United Nations Convention against Transnational Organized Crime of 2000

Considering the nature and characteristics of telematic technology, the form of crime that related to such technology has also the same transnational character. In line with the efforts in preventing, minimizing and combating trans-national crime in the field of telematic, it is very timely to discuss this Convention as it also regulate aspects of international cooperation. International cooperation is becoming more important considering the rapid increase in trans-national organized crime that involves international criminal groups.

Some important provisions in the context of international cooperation covers:

- Principles of international cooperation, such as sovereign equality and territorial integrity[19];
- Criminalizing crime that involve organized criminal group[20];
- Criminalizing money laundering, including cyberlaundering[21];
- Criminalizing crime of Corruption[22];
- International cooperation in conducting confiscation[23];
- Implementation of jurisdiction by State Parties[24].
- Extradition issues[25];
- Transfer of sentenced persons[26];
- Mutual legal assistance in criminal matters[27];
- Measures to enhance cooperation law enforcement authorities[28];
- Etc.

2. Developing National Legal Instrument that meet International Standards

[18]For further analysis and elaboration, see James K Robinson, "Internet as the Scene of Crime". Paper presented before International Computer Crime Conference, Oslo- Norway, 29-31 May 2000, page 9.

[19]See United Conventions against International Organized Crime of 2000, article 4.
[20]Ibid, article 5.
[21]Ibid, article 6 and 7.
[22]Ibid, article 8 and 9.
[23]Ibid, article 13.
[24]Ibid, article 15.
[25]Ibid, article 16.
[26]Ibid, article 17.
[27]Ibid, article 18.
[28]Ibid, article 26.

In an interdependent global community, the development of national legislation that meets International Standards or at least follow International common practices and best practices, is an unavoidable requirement. In the situation where substantive aspects of national law has meet existing International Standards in force, it will eventually ease its International relations of both among legal entities (corporations) and/or individuals of that country, including for its International transactions.

Efforts in standardizing national law rules and principles, for the purpose prevention, minimizing and combating cybercrime can be conducted by way of:

a. Adopting relevant international legal principles and/or instruments which would be able to accommodate national interest by way of ratification or accession;

b. Formulating national legislation by taking into consideration relevant existing international legal instruments, both hard laws and soft laws.

B. Aspects of International Cooperation on Law Enforcement

1. Extradition

The problem of extradition concerning certain forms of international crime is quite a complicated issue. It is not only from the fact that the variety of crime are increasing, but also caused by some limitations in the implementation of extradition, even though there are several international legal instruments in place, both bilateral, regional or multilateral. As a way to enhance international cooperation on extradition, first of all there is a need to accurately identify what sort of national interest that should be accommodated. Further in what way existing national laws and regulations impose some limitations to the process finalizing cooperation in the field of extradition. In addition, observation shall be conducted on the on going development in international arena, including in the field of cybercrime, in order to formulate extraditable offences in a more comprehensive and detail way.

To take further steps in promoting international cooperation concerning extradition of cybercriminals, it is necessary to examine existing national laws and

regulations on extradition and also Indonesian experience in formulating extradition treaties with some other countries. The existing Law on Extradition which is still in force and have been used as reference in concluding extradition treaties is Law No 1 of 1979 on Extradition. The Law regulates certain basic provisions[29], such as: general provisions; principles of extradition[30]; extradition procedures either as requesting country or requested country[31]; transitional provisions[32]; concluding provisions[33]; and also equipped with annex, which contain list of extraditable offences[34].

Based on my observation on list of extraditable offences under Law no 1 of 1979 concerning Extradition, it seems that new types of crimes as recently arise, including cybercrime, are not covered by the Law. In several bilateral extradition treaties, inter alia with Australia, the number of extraditable offences have been added to reach the total number of about 33 extraditable offences[35], even though it still not cover new types of offences. For the above reason, in order to enhance international cooperation, especially regarding extradition for cybercriminals, it is recommended to revise Law No 1 of 1979 concerning Extradition by taking into consideration relevant international treaties, including the possibility to ratify both Convention on Cybercrime and Convention on International Organized Crime.

2. Mutual Legal Assistance in Criminal Matters

In the efforts to prevent and combat cybercrime, particularly in the context of international cooperation, the existence of bilateral agreement on mutual legal assistance on criminal matters and other national laws is absolutely important.

Law no 1 of 2006 concerning Mutual Legal Assistance on Criminal Matters has laid down some legal basis for handling transnational crime. It gives emphasis on the importance of international cooperation in providing mutual legal assistance on criminal matters[36]. In the framework of providing mutual legal assistance on criminal matters, this Convention provides legal recognition of statement or document even if in the form of electronic

[29]Among other on definition of extradition, for further detail see Law No 1 of 1979 concerning Extradition, Chapter I article 1.
[30]See Ibid, article 2-17.
[31]See Ibid, Chapter III-X, article 18-46.
[32]Ibid, Chapter XI, article 47.
[33]Ibid, Chapter XII, article 48.
[34]See Annex to Law No 1 of 1979, in such annex, there are about 32 extraditable offences.
[35]For further detail, see article 2 of Extradition Treaty between The Republic of Indonesia and Australia dated 22 April 1992 which has been ratified by Law No 8 of 1994.
[36]See considerations of Law No 1 of 2006 concerning Mutual Legal Assistance on Criminal Matters.

record[37]. Thus, it can be used to uncover cybercrime cases. The mutual legal assistance covers the whole process, from investigations, prosecution to court proceedings[38].

C. Cooperation for Preventing and Overcoming Cyberpornography

The problem of pornography, particularly cyberpornography that use cyberworld as its media requires special attention, mainly to protect the children. Some developed countries like USA, United Kingdom, etc., have sufficiently provides relevant legal framework, including laws and regulations that protect children from child pornography. It reflects serious attention from their governments to prevent and combat cyberpornography, particularly child pornography via internet.

At the international level international cooperation to prevent and combat childpornography has become an absolute requirement to be consistently implemented in order to protect young generation from irresponsible cybercriminals. In that respect it is interesting to observe the statement of Eric Holder, US Deputy Attorney General at International Conference Combating Child Pornography on the Internet. He among other stated :

"Child pornography on the internet must be issue of international concerns, it must be at the forefront of the global agenda. Children are our most precious and fragile resource, they are our futures, this is true regardless of what nation they come from. Their protection must be an international priority"[39].

Some recommended steps for international cooperation, including but not limited to:

1. Efforts to criminalise cyberpornography;
2. The need for the same understanding on the scope of cyberpornography;
3. Facilitating law enforcer efforts, including via Interpol;
4. Standardizing preventive measures;
5. More intensive interaction among central authority in preventing and combating cyberpornography;
6. Developing procedure for discovery and investigations;
7. Optimizing mutual legal assistance on criminal matters, especially on cyberpornography;
8. Promote effectiveness of extradition process for cybercriminals;
9. Efforts to overcome conflict of laws.

[37]See, Ibid, article 1 paragraphs 2 and 3.
[38]Ibid, article 3.
[39]See Eric Holder, Ibid, page 1.

IV. Concluding Remarks

Based on previous elaboration and analysis, some conclusions and recommendations can be drawn, namely:

1. The increasing quantity, intensity, quality and modus operandi of cybercrime may raise new problems for its prevention and efforts to combat it;
2. Cyber pornography as one aspect of cybercrime and in particular child pornography via internet require special attention in order to protect public morality in general and in particular the future of the children;
3. By taking into consideration the characteristics and ongoing development of cybercrime, international cooperation is absolutely required;
4. Promotion of International Cooperation in preventing and combating cybercrime and cyberpornography will be conducted based on mechanism and best practices both at international level, regional, and bilateral and in accordance with relevant sources of law;
5. In the efforts to enhance effectiveness of International Cooperation, for Indonesia there is a need to institutionalize national legislation that meet international standards, both from its scope of substances and procedures;
6. There is a need to harmonise national legislation relevant to cybercrime and cyberpornography with existing laws both at national and international level.

Selected Bibliography

A. Books and Articles

- Akdeniz Yaman (ed), The Internet, Law and Society, Pearson Education Ltd, Essex, UK, 2000;
- Arief, Barda Nawawi, Tindak Pidana Mayantara: Perkembangan Kajian Cybercrime di Indonesia, Raja Grafindo Persada, Jakarta, 2006;
- Atmasasmita, Romli, "International Cooperation on Combating Human Trafficking Especially Women and Children: A View from Indonesia", Indonesian Journal of International Law, Vol 1 No 4, July 2004;
- Bowrey, Kathy, Law and Internet Culture, Cambridge University Press, 2005;
- Evans, Malcolm D, International Law Document, Oxford University Press, Seventh Edition, 2005;
- Gregory, Kevin D, "Fighting Cybercrime What are the Challenges Facing Europe", Statement before European Parliament, 19 September 2000;

- Gringas, Clive, The Laws of the Internet, Butterworth, London, 1997;
- Halbert terry & Elaine Ingulli, Cyber Ethics, Second edition, Thomson Corporation, USA, 2005;
- Indradi, Ade Ary Sam, Carding, Modus Operandi, Penyidikan dan Penindakan, Grafika Indah, Jakarta, 2006;
- Irsan, Koesparmono, dkk, Pengkajian Hukum tentang Masalah Kekuatan Hukum Alat Bukti Elektronik, Badan Pembinaan Hukum Nasional, Jakarta, 1996/1997;
- Lim, Yee Fen, Cyberspace Law, Commentaries and Materials, Oxford University Press, 2002;
- Makarim, Edmond, Kompilasi Hukum Telematika, Raja Grafindo Persada, Jakarta, 2003;
- Mares, radu (ed), Business and Human Rights, A Compilation of Documents, Martinus Nijhoff Publishers, Leiden, The Netherlands, 2004;
- Mubarak, Ali, "Urgensi Cyberlaw and Cybercrime", Bisnis Indonesia, 26 August, 2006;
- Munir, Abubakar, "Cybercrime: The National and International Legal Initiatives", unpublished;
- Reksodiputro, Mardjono, "Kejahatan Korporasi Sustu Fenomena Lama dalam Bentu Baru", Indonesian Journal of International Law, Volume 1 no 4, 2004;
- Robinson, James K, "Internet as the Scene of Crime", paper presented at the Conference on International Computer Crime, Oslo, 29-31 May 2000;
- Rosenoer, Jonathan, Cyberlaw, The Law of the Internet, Springer Verlag, New York Inc, 1997;
- Rowland, Diane & Elizabeth Macdonald, Information Technology Law, Cavendish Publishing Limited, London, 1997;
- Sitompul, Asriel, Hukum Internet: Pengenalan Mengenai Masalah Hukum di Cyberspace, Citra Aditya Bakti, Bandung, 2001;
- Supancana, I.B.R, "Cybercrime: Law and Regulatory Issues", Course Materials for Post Graduate Program, Multimedia Management, Pelita Harapan University, 2005, Unpublished;
- Supancana, I.B.R, Law and Regulatory Aspects of Multimedia, reading Materials, Post Graduate Study, Multimedia Management, Pelita Harapan University, Jakarta, 2005, Unpublished;

- Supancana, I.B.R, Cyberlaw and Cyber Ethics: Kontribusinya bagi Dunia Bisnis, Post Graduate Study, Master of Management Program, Universitas Airlangga, Surabaya, 2005; Unpublished;
- Wallace, Jonathan, Sex, Laws and Cyberspace, Henry Holt and Company, New York, 1996;
- Zulhuda, Sonny, "Cyberlaw and Enforcement";
- Zulhuda, Sonny, "Computer Crimes in Malaysia";
- Zulhuda, Sonny, "Information Security Law";
- Zulhuda, Sonny, "Keadilan dibalik telekonferensi".

B. Relevant National Laws and Regulations

- Law No 1 of 1979 concerning Extradition;
- Law No 1 of 1999 concerning Ratification of Treaty between The Republic of Indonesia and Australia on Mutual Assistance in Criminal matters;
- Law No 36 of 1999 concerning Telecommunication;
- Law No 37 of 1999 concerning International Relations;
- Law No 24 of 2000 concerning International Treaty;
- Law No 1 of 2006 concerning Mutual Legal Assistance on Criminal matters.

C. Relevant International Legal Instruments

- Council of Europe Convention on Cybercrime, Budapest, 2001;
- The Palermo Convention against Trans-national Organized Crime of 2000;
- Council of Europe Convention on the prevention of Terrorism of 2005.