REFORMATION OF LAW ENFORCEMENT OF CYBER CRIME IN INDONESIA

Bambang Tri Bawono
Sultan Agung Islamic University
bambang@unissula.ac.id

Abstract

Technological progress and the presence of globalization in third world countries including Indonesia has a variety of consequences, this includes the negative impact of increasing cyber crime in Indonesia. Increasing cyber crime in the community with a variety of increasingly sophisticated modus operandi, in reality is not balanced by the existence of a comprehensive legal umbrella and also the absence of adequate facilities and pre-facilities is a separate issue in the enforcement of cyber crime cases in a dynamic society. Enforcement weaknesses are the lack of human resources of investigators who understand cyber crime, and the lack of means and pre-law enforcement facilities in cyber crime. so it is necessary to increase the HR of the relevant law enforcers as well as the improvement of facilities and pre-facilities related to law enforcement in cyber crime. enforcement weaknesses are the lack of human resources of investigators who understand cyber crime, and the lack of means and pre-law enforcement facilities in cyber crime. so it is necessary to increase the HR of the relevant law enforcers as well as the improvement of facilities and pre-facilities related to law enforcement in cyber crime.

Keywords: *Cyber Crime; Law Enforcement; Legal Reform.*

A. INTRODUCTION

Cybercrime is one of the dark sides of technological advances that have a very broad negative impact on all fields of modern life today. With the advancement of technology, it is easy for some people to enter the scope of crime simply by relying on their ability to drive the technological system. The problem of cyber crime in its development is inseparable from the problem of computer network security or internet-based information security in the current era of globalization, this can be observed even more clearly by viewing the problem of information as a commodity. Information as a commodity has consequences in the form of the need for reliability in services related to technology-based information. To achieve the level of reliability of course the information itself must always be updated so that the information presented is not out of date. The dilemma arises when the growth of technology-based information together with the growth of new crimes, cyber crime is a crime that arises along with the rapid development of information technology.

Relating to cybercrime in Indonesia, until this time the majority of cybercrime has not been regulated in a clear legal norms in the

legislation, because it was in prosecuting cybercrime applied the provisions of the Criminal Code and the provisions of the Act beyond the Criminal Code. The provisions in the Criminal Code that can be used to prosecute cybercrime by way of interpretation, extensive is the provision on the crime of counterfeiting (as stipulated in Article 263 to Article 276), the crime of theft (under Article 362 up to 367), the crime of fraud (as under Article 378 up to 395), and the crime of destruction of goods (as stipulated in Article 407 through Article 412).[1]

Integration in existing regulations means making savings and preventing over criminalization As a preventive measure for all matters relating to criminal offenses in the field of computers, especially cyber, as far as possible is returned to the existing legislation, namely the Criminal Code (the Criminal Law Book) and regulations outside the Criminal Code. Integration in existing regulations means making savings and preventing over criminalization As a preventive measure for all matters relating to criminal offenses in the field of computers, especially cyber, as far as possible is returned to the existing legislation, namely the Criminal Code (the Criminal Code) and regulations outside the Criminal Code. Integration in existing regulations means making savings and preventing over criminalization[2], without changing the principles that apply and does not cause side effects that can interfere with the development of information technology. This gives the consequence that legal politics related to cyber crime must be specifically regulated.[3] In its development, regulations related to cyber crime are regulated in:

1. Law Number 19 of 2002 concerning Copyright
2. Law Number 36 of 1999 concerning Telecommunications
3. Law Number 8 of 1997 concerning Company Documents
4. Law Number 25 of 2003 concerning Amendments to Law Number 15 of 2002 concerning Money Laundering
5. Law Number 15 of 2003 concerning Eradication of Terrorism Crimes
6. Law Number 11 of 2008 concerning Information and Electronic Transactions.

B. DISCUSSION

1. Weaknesses in Law Enforcement in Cyber Crimes

Crimes that are closely related to the use of computer-based technology and telecommunications networks are grouped in several forms

1 Andri Winjaya Laksana, Cybercrime Comparison Under Criminal Law In Some Countries, *Jurnal Pembaharuan Hukum*, Vol V No.2 April-Agustus 2018, P.217-226

2 Marjono Reksodiputro, *Progress of Economic Development and Crime*, Center for Justice and Legal Service, Jakarta, 1994, P. 13

3 Sri Endah Wahyuningsih, Rismanto, Kebijakan Penegakan Hukum Pidana Terhadap Penanggulangan Money Laundering Dalam Rangka Pembaharuan Hukum Pidana Di Indonesia, *Jurnal Pembaharuan Hukum*, Vol. II No. 1 Januari - April 2015, P.46-56.

according to the existing modus operandi, namely:[4]

a. *Unauthorized Access to Computer Systems and Services*

Crimes committed by entering / breaking into a computer network system illegally, without permission or without the knowledge of the owner of the computer network system that he entered Usually the perpetrators (hackers) do it with the intention of sabotage or theft of important and confidential information. However, there are also those who do it only because they feel challenged to try their expertise to penetrate a system that has a high level of protection. This crime is increasingly widespread with the development of Internet / intranet technology. We certainly have not forgotten that when the East Timor problem was warmly discussed at the international level, several Indonesian government-owned websites were damaged by hackers (Kompas, 11/08/1999). Some time ago, hackers have also successfully penetrated into the data base containing the data of the users of America Online (AOL), a United States company engaged in e-commerce that has a high level of confidentiality (Indonesian Observer, 6/26/2000). The site of the Federal Bureau of Investigation (FBI) is also not spared from hacker attacks, which results in the inability of this site for some time;

b. *Illegal Contents*

It is a crime to enter data or information on the Internet about something that is not true, unethical, and can be considered unlawful or disturbing public order. For example, the loading of a hoax or slander that will destroy the dignity or dignity of others, matters relating to pornography or the loading of information which is state secrets, agitation and propaganda to fight legitimate government and so on;

c. *Forgery Data*

It is a crime to falsify data on important documents stored as scripless documents over the Internet. This crime is usually directed at e-commerce documents by making it appear as if there was a "typo" which will ultimately benefit the offender because the victim will enter personal data and credit card numbers that can be misused;

d. *Cyber Espionage*

It is a crime that utilizes the internet network to conduct spy activities against other parties, by entering the computer network system of the target party. This crime is usually directed against business rivals whose important

4 Abdul Wahid and Mohammad Labib, *Kejahatan Mayantara*, Refika Aditama, Bandung, 2005, p. 56

documents or data (data base) are stored in a computerized system (connected to a computer network);

e. *Cyber Sabotage and Extortion*

This crime is done by making interference, destruction or destruction of data, computer programs or computer network systems that are connected to the Internet. Usually this crime is committed by infiltrating a logic bomb, computer virus or a certain program, so that data, computer programs or computer network systems cannot be used, do not run as they should, or run as desired by the perpetrators;

f. *Offense against Intellectual Property*

This crime is directed against intellectual property rights owned by other parties on the Internet. For example, impersonation on the web page of a site belonging to someone else illegally, broadcasting information on the Internet that turns out to be someone else's trade secret, and so on;

g. *Infringements of Privacy*

This crime is usually directed against a person's personal information stored on a computerized personal data form, which, if known by others, can harm the victim materially or immaterial, such as credit card numbers, ATM PIN numbers, disabilities or hidden diseases and so on.

In its development there are some positive laws that are generally applicable and can be imposed on cyber criminals, especially for cases that use computers as a means, including:

1) Criminal Code

In an effort to handle cases that occur investigators carry out analogies or parables and similarities to the Articles contained in the Criminal Code. Articles in the Criminal Code are usually used more than one Article because they involve several acts at once Articles that can be imposed in the Criminal Code on cyber crime include:[5]

a) Article 362 of the Criminal Code is imposed for carding cases where the offender steals credit cards numbers belonging to other people even though not physically because only the card numbers are taken by using a card generator software on the Internet to conduct transactions in ecommerce. After the transaction is

5 Bulletin of Banking and Central Banking Laws, Development of Cyber Crimes and Their Mitigation Efforts in Indonesia by POLRI, Volume 4 No. 2, August 2006.

done and the goods are sent, then the seller who wants to withdraw his money at the bank turns out to be rejected because the card owner is not the person who made the transaction.

b) Article 378 of the Criminal Code can be charged for fraud as if offering and selling a product or goods by placing advertisements on one website so that people are interested in buying it and then sending money to advertisers. But, in fact, the item does not exist. This is known after the money is sent and the ordered goods do not arrive, so the buyer becomes deceived.

c) Article 335 of the Criminal Code can be imposed on cases of threats and extortion carried out by e-mail sent by the perpetrators to force the victim to do something in accordance with what the perpetrator wants and if it is not carried out it will have a harmful impact. This is usually done because the perpetrator usually knows the secret of the victim.

d) Article 311 of the Criminal Code may be imposed for cases of defamation using the Internet media. The mode is the perpetrator to spread e-mails to victims' friends about a story that is not true or send an e-mail to a mailing list so that many people know the story.

e) Article 303 of the Criminal Code may be imposed to ensnare gambling games conducted online on the Internet with organizers from Indonesia.

f) Article 282 of the Criminal Code can be imposed for the spread of pornography and pornographic websites which are widely circulated and easily accessed on the Internet. Although speaking Indonesian, it is very difficult to crack down on the culprit because they registered the domain abroad, where pornography featuring adults is not illegal.

g) Articles 282 and 311 of the Criminal Code may be imposed for cases of distribution of personal photographs or films of someone who is vulgar on the internet, for example the Sukma Ayu-Bjah case.
h) Article 378 and 262 of the Criminal Code can be imposed on carding cases, because the perpetrators commit fraud as if they want to buy an item and pay with a credit card whose credit card number is stolen.
i) Article 406 of the Criminal Code may be imposed on cases of deface or hacking that make other people's systems, such as websites or programs, malfunction or can be used properly.

2) Law Number 19 of 2002 concerning Copyright

A computer program is a collection of instructions that is realized in the form of language, code, schema or other forms which, when combined with media that can be read by a computer, will be able to make the computer work to perform special functions or to achieve specific results, including preparation in designing instructions -the construction.[6]

Copyright for computer programs is valid for 50 years. The price of computer / software programs which are very expensive for Indonesian citizens is a promising opportunity for business people to duplicate and sell pirated software at very cheap prices. For example, an anti-virus program for $ 50 can be purchased for Rp. 20,000.00. Sales at very cheap prices compared to the original software generate huge profits for the perpetrators because the capital spent is not more than Rp. 5,000.00 per piece. The rise of software piracy in Indonesia that seems "understandable" is certainly very detrimental to copyright owners.

3) Law Number 36 of 1999 concerning Telecommunications

According to Article 1 number (1) of Law No. 36 of 1999: "Telecommunications is every transmission, transmission and / or reception and any information in the form of signs, signals, writing,

6 Article 1 number (8) of Law No. 19 of 2002 concerning Copyrights.

pictures, sounds and sounds through a wire system, optics, radio or other electromagnetic systems. "

From this definition, the Internet and all its facilities are a form of communication because they can send and receive any information in the form of images, sound or film with an electromagnetic system. Misuse of the Internet that interferes with public or private order may be subject to sanctions by using this Law, especially for hackers who enter other people's network systems as stipulated in Article 22, namely that every person is prohibited from carrying out acts without rights, illegals, or manipulating :

a) Access to telecommunications networks
b) Access to telecommunications services
c) Access to specialized telecommunications networks

If you do this as happened on the KPU website,[7] Article 50 may be imposed which reads "Whoever violates the provisions referred to in Article 22, shall be liable to a maximum imprisonment of 6 (six) years and / or a maximum fine of Rp. 600,000,000.00 (six hundred million rupiah)".

4) Law Number 8 of 1997 concerning Company Documents

With the issuance of Law No. 8 of 1997 dated March 24, 1997 concerning Company Documents, the government is trying to regulate the recognition of microfilms and other media (non-paper information storage devices and have a level of security that can guarantee the authenticity of documents transferred or transformed, for example Compact Disk - Read Only Memory (CD-ROM), and Write-Once-Read-Many (WORM), which are regulated in Article 12 of the Law as valid evidence.

5) Law Number 25 of 2003 concerning Amendments to Law Number 15 of 2002 concerning Money Laundering

Money laundering is a process or act that aims to conceal or disguise the origin of money or assets obtained from criminal activities which are then converted into assets that appear to originate from legitimate activities. In accordance with Article 2 of Law No. 15 of 2002, criminal acts that trigger money laundering include corruption, bribery, smuggling of goods / labor

7 www.kpu.go.id. Accessed March 3, 2010.

/ immigrants, banking, narcotics, psychotropic, slave / woman / child / illicit trafficking, abduction, terrorism, theft, embezzlement and fraud.[8]Money laundering activities have a serious impact on the stability of the financial system and the economy as a whole. Money laundering is a multi-dimensional and transnational crime that often involves a large amount of money.

This Law also regulates electronic evidence in accordance with Article 38 letter b, which is other evidence in the form of information that is spoken, sent, received, or stored electronically by optical devices or similar.

6) Law Number 15 of 2003 concerning Eradication of Terrorism Crimes

In addition to Law No. 25 of 2003, this Law regulates electronic evidence in accordance with Article 27 letter b, which is other evidence in the form of information that is spoken, sent, received, or stored electronically with optical devices or similar. Digital evidence or electronic evidence is very instrumental in investigating terrorism cases, because at this time communication between the perpetrators in the field with their leaders or intellectual actors is done by utilizing facilities on the Internet to receive orders or convey conditions on the ground because the perpetrators find tracking of the Internet more difficult compared to tracking via cellphone.

7) Law Number 11 of 2008 concerning Information and Electronic Transactions.

The ITE Law is perceived as cyberlaw in Indonesia, which is expected to regulate all matters of the Internet (cyber), including giving punishment to cybercriminals. Cybercrime is detected from two points of view:

a) Crimes Using Information Technology as Facilities: Piracy, Pornography, Counterfeiting / Credit Card Theft, Email Fraud, Spam Emails, Online Gambling, Internet Account Theft, Terrorism, Sara Issues, Misleading Sites,
b) Crimes That Make Information Technology Systems

8 Article 2 paragraph (1) letter q of Law Number 25 of 2003 concerning Amendments to Law Number 15 of 2002 concerning Money Laundering Crimes.

A Target: Theft of Personal Data, Creation / Spread of Computer Viruses, Hacking / Piracy of Sites, Cyberwar, Denial of Service (DOS), Crimes Related to Domain Names.

In its development, cyber crime has become an interesting and sometimes difficult issue because:

a) The activities of the cyber world are not limited by state territories;
b) The activities of the cyber world are relatively intangible;
c) The difficulty of proof because electronic data is relatively easy to be changed, tapped, falsified and sent to all parts of the world in seconds;
d) Copyright infringement is possible technologically;
e) It is no longer possible to use conventional law. The analogy of the problem is similar to the shock of conventional law and the apparatus when electricity was initially stolen. The stolen evidence is not possible to go down to the courtroom. Likewise, if there is cyber crime, band width theft.

In general, based on the above explanation, it can be concluded that the ITE Law may be called a cyberlaw because the content and wide scope discusses the regulation in cyberspace, although on some sides there are some that are not too straightforward and some are also slightly missed. The contents of the ITE Law if summarized are as follows:

a) Electronic signatures have the same legal power as conventional signatures (wet and stamped ink). In accordance with the e-ASEAN Framework Guidelines (recognition of cross-border digital signatures);
b) Electronic evidence is recognized as any other evidence provided for in the Criminal Code;
c) The ITE Law applies to every person who commits legal actions, both within Indonesia and outside Indonesia who have legal

consequences in Indonesia;

d) Domain Name Settings and Intellectual Property Rights;
e) Prohibited acts (cybercrime) are explained in Chapter VII (articles 27-37), which are as follows:
   i. Every person intentionally and without the right to distribute and / or transmit and / or make access to Electronic Information and / or Electronic Documents that have contents that violate decency;
   ii. Every person intentionally and without the right to distribute and / or transmit and / or make access to Electronic Information and / or Electronic Documents that have gambling contents;
   iii. Any person intentionally and without the right to distribute and / or transmit and / or make access to Electronic Information and / or Electronic Documents that have content of defamation and / or defamation;
   iv. Any person intentionally and without the right to distribute and / or transmit and / or make accessible Electronic Information and / or Electronic Documents that have extortion and / or threatening contents;
   v. Everyone intentionally and without the right to spread false and misleading news that results in consumer losses in Electronic Transactions;
   vi. Every person intentionally and without the right to disseminate information intended to incite hatred or hostility of certain individuals and / or groups of people based on ethnicity, religion, race and intergroup (SARA);
   vii. Every person intentionally and without right sends Electronic

Information and / or Electronic Documents that contain threats of violence or intimidation that are addressed in person. People intentionally and without rights or unlawfully accessing other people's Computers and / or Electronic Systems in any way;

viii. Every person intentionally and without right or unlawfully accesses Computers and / or Electronic Systems in any way for the purpose of obtaining Electronic Information and / or Electronic Documents. Any person who intentionally and without rights or unlawfully accesses Computers and / or Electronic Systems in any way by violating, breaking through, surpassing, or breaking into security systems;

ix. Every person intentionally and without rights or unlawfully conducts interception or wiretapping of Electronic Information and / or Electronic Documents in a particular Computer and / or Electronic System belonging to another Person. Every person intentionally and without right or unlawfully intercepts the transmission of Electronic Information and / or Electronic Documents that are not public from, to, and in a particular Computer and / or Electronic System that belongs to another Person, whether that does not cause any changes nor does it cause changes, omissions, and / or termination of Electronic Information and / or Electronic Documents that are being transmitted. Except

interception interception carried out in the context of law enforcement at the request of the police, prosecutors,

x. Every person intentionally and without rights or against the law in any way changes, adds, subtracts, transmits, damages, removes, transfers, hides an Electronic Information and / or Electronic Documents belonging to another person or public property. Any person intentionally and without rights or against the law in any way transferring or transferring Electronic Information and / or Electronic Documents to the Electronic System of another unauthorized person;

xi. For acts that result in the disclosure of confidential Electronic Information and / or Electronic Documents which are accessible to the public with improper data integrity;

xii. Every person intentionally and without rights or unlawfully takes any action that results in disruption of the Electronic System and / or causes the Electronic System to not work properly. Everyone intentionally and without rights or against the law produces, sells, procures for use, imports, distributes, provides or owns:
   a. Computer hardware or software designed or specifically developed to facilitate the acts referred to in Article 27 to Article 33;
   b. password through a Computer, Access Code, or similar thing intended to make the Electronic System

accessible for the purpose of facilitating acts referred to in Article 27 to Article 33. (2) The actions referred to in paragraph (1) are not criminal if intended to conduct research activities, testing the Electronic System, for the protection of the Electronic System itself legally and not against the law.

xiii. Every person intentionally and without right or unlawfully manipulates, creates, changes, omits, destroys Electronic Information and / or Electronic Documents in order that the Electronic Information and / or Electronic Documents are considered as if the data is authentic;

xiv. Every person intentionally and without rights or unlawfully commits acts as referred to in Article 27 to Article 34 which results in harm to others Article 37 Every person intentionally commits prohibited acts as referred to in Article 27 to Article 36 outside the territory of Indonesia against the Electronic System within the jurisdiction of Indonesia.

In its development, the weaknesses found in the investigation process include the following:

a) Inadequate legal instruments

Weak legislation that can be applied to cybercrime perpetrators, while the use of articles contained in the Criminal Code is often still quite doubtful for investigators. The law governing cybercrime refers to the Law of the Republic of Indonesia Number 36 of 1999 concerning Telecommunications as well as not yet fully regulating various types

of cyber crime, for example trafficking in people through internet facilities.

b) Investigator ability

In general, police investigators are still very minimal in mastery of computer operations and understanding of computer hacking and the ability to conduct investigations of these cases. Some very influential factors (determinants) are:

1) Lack of knowledge about computers.
2) Technical knowledge and experience of investigators in handling cybercrime cases is still limited.
3) Proof system factors that make investigators difficult.

c) Evidence

Issues of evidence encountered in the investigation of Cybercrime, among others, are related to the characteristics of cybercrime crime itself, namely:

1) Cybercrime targets or media are data and or computer systems or internet systems that are easily changed, deleted, or hidden by the culprit. Therefore, data or computer systems or the internet relating to the 25 crimes must be recorded as evidence of the crimes that have been committed. Problems arise related to the position of the recording media (recorder) that KUHAP has not recognized as valid evidence;
2) The position of victim witnesses in cybercrime is very important because cybercrime is often carried out almost without witnesses. On the other hand, victim witnesses are often far away abroad, making it difficult for investigators to examine witnesses and file the results of investigations. Public prosecutors also do not want to accept case files that are not equipped with Witness Examination Reports, especially

victim witnesses and must be equipped with Witness Spilling Minutes due to it is probable that the witness could not be present at the trial given the witness' residence. This results in a lack of valid evidence if the case file is submitted to the court for trial so that the risk of the defendant will be declared free.

At this time, the problem that is considered the most urgent is the regulation of the position of legal evidence for some evidence that is often found in Cybercrime such as data or system programs stored on diskettes, hard disks, chips, or other media recorders.

d) Forensic computer facilities

In order to prove the traces of hackers, crackers and phreackers in carrying out their actions, especially those related to computer programs and data, Polri's facilities were inadequate because there were no forensic computers. This facility is needed to uncover digital data and record and store evidence in the form of soft copies (images, programs, etc.). In this case the National Police still do not have adequate forensic computing facilities.[9]

2. Law Enforcement Reform in Cyber Crime

In its development in order to be able to realize fair cyber crime law enforcement, it is necessary to do several things, namely:

a. Special laws need to be made to regulate cyber crime, with special cyber crime laws governed, issues of technological progress will not be able to hamper the course of the law, as for the law-making process according to David Eastonthat the drafting of a legal rule is inseparable from the personal influence that has the authority to create the legal regulations both individuals and groups, in addition to the person, the environment in the form of a social, economic, political, cultural, security and geographic environment as well as the effects of the judicial,

9 Paper of Drs. Rusbagio Ishak (Kombes Pol / 49120373), Central Java Regional Police Serse Kadit, at a seminar on Hacking held by NeoTek Magazine in August 2002 in Semarang

legislative, and executives and community leaders and so on are also factors that influence the input of a legal regulation drafting. These factors interact with each other so that changing inputs into outputs in the process of drafting legal regulations.[10]

b. In handling cybercrime cases, investigators who are experienced (not beginner investigators) are needed, their education is directed at mastering technical investigations and investigating administration as well as the basics of knowledge in the computer and hacker profiles, this has been alluded to above which states that, John Sulivan with the theory of Well MES said that the requirements to obtain good law enforcement must rest on three things, namely:[11]

1) *Well Motivation*

Well Motivation one must see the motivation of someone to devote themselves as law enforcement and lawmakers. From the start, a candidate for law enforcement and lawmakers must know and be motivated that being a matter of law enforcement is a challenge as well as a difficult task. In this aspect, law enforcers must have a motivation that aims not only at the interests of law enforcers, but more than that also protects victims of cyber crime.

2) *Well Education*

Well Education, meaning that an enforcer and law maker should meet certain educational standards. So that in addition to formal education other education is also needed related to knowledge of law, for example legal seminars and short courses. In this aspect, every law enforcement officer related to cybercrime issues must be able to be educated in depth and fair with the knowledge of law that continues to develop along with the times and technology.[12]

3) *Well Salary*

Well Salary, This means that salaries of law enforcers and

10 Hasyim Azzizurahman, Pembaharuan Kebijakan Hukum Pidana di Era Cyber, *Masalah-Masalah Hukum*, Jilid 41, Nomor 2, Tahun 2012, P.298-305.

11 Ali Mansyur, Legal Institutions and Enforcement in Indonesia, Sultan Agung Islamic University, Semarang, 2010, P. 83-84

12 Marheni Dharyadi Siwi , Siswandari, Gunarhadi, The Correlation between Leadership, Motivation, Work Climate and High Economic Teachers' Performance in Karanganyar Regency, *International Journal of Active Learning*, Vol. 4 (1) (2019),P.45-58

lawmakers must be considered so that in carrying out their duties properly, law enforcers and lawmakers are not charged with the costs of carrying out their duties. So as far as possible avoid law enforcers and loaders with the dilemma that is the small salary and the lack of operational funds that make law enforcement losers.

c. The forensic computing facility that will be established by the National Police is expected to be able to serve three important things, namely evidence collection, forensic analysis, expert witness.

In order for this whole solution to be carried out well, several things are needed, some of which Yahezkel states that aif you want to see law as a system, then law enforcement as a process will involve a variety of interconnected components and some even have a fairly close dependency. As a result, the absence of one component can lead to inefficient and useless so that the goal of the law aspired is difficult to realize. These components include personnel, information, budget, substantive law facilites, procedural law, decision rules and decision habits.

C. CONCLUSION

Based on various explanations above, it is clear that several things can be concluded, The implementation of law enforcement in cyber crime currently in Indonesia has several weaknesses, namely weakness in legal regulations that have not thoroughly governed the types of cyber crime, weaknesses in enforcement, namely the lack of human resources investigators who understand cyber crime, and the lack of facilities and pre-law enforcement facilities in cyber crime. so it is necessary to increase the HR of the relevant law enforcers as well as the improvement of facilities and pre-facilities related to law enforcement in cyber crime.

BIBLIOGRAPHY

Book:

Abdul Wahid and Mohammad Labib, 2005, Kejahatan Mayantara, Refika Aditama, Bandung;

Ali Mansyur, 2010, Legal Institutions and Their Enforcement in Indonesia, Sultan Agung Islamic University, Semarang;

Andri Winjaya Laksana, Cybercrime Comparison Under Criminal Law In Some Countries, Jurnal Pembaharuan Hukum, Vol V No.2 April-Agustus 2018;

Marjono Reksodiputro, 1994, Progress of Economic Development and Crime, Center for Justice and Legal Service, Jakarta;

Bulletin of Banking and Central Banking Laws, Development of Cyber Crimes and Their Mitigation Efforts in Indonesia by POLRI, Volume 4 No. 2, August 2006.

Central Java Tribune, Crimes in the Cyber World Increases, Central Java Tribune Edition 10 May 2016;

Hasyim Azzizurahman, Pembaharuan Kebijakan Hukum Pidana di Era Cyber, Masalah-Masalah Hukum, Jilid 41, Nomor 2, Tahun 2012;

Head of Information V and Cyber Crime Unit of the Indonesian Police Headquarters Criminal Investigation Agency, Kombespol Dr. Peter Golose;

Marheni Dharyadi Siwi, Siswandari, Gunarhadi, The Correlation between Leadership, Motivation, Work Climate and High Economic Teachers' Performance in Karanganyar Regency, International Journal of Active Learning, Vol. 4 (1) (2019);

Paper of Drs. Rusbagio Ishak (Kombes Pol / 49120373), Central Java Regional Police Serse Kadit, at a seminar on Hacking held by NeoTek Magazine in August 2002 in Semarang;

Sri Endah Wahyuningsih, Rismanto, Kebijakan Penegakan Hukum Pidana Terhadap Penanggulangan Money Laundering Dalam Rangka Pembaharuan Hukum Pidana Di Indonesia, Jurnal Pembaharuan Hukum, Vol. II No. 1 Januari - April 2015;