International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

# Emerging Issue in Cyber Crime: Case Study Cyber Crime in Indonesia

**Henry Kristian Siburian**

Head of Quality Assurance,, STMIK Budidarma,, Jl. Sisingamangaraja XII No.338, SitiRejo I, Medan Kota, Kota Medan, Sumatera Utara 20216, Indonesia

**Abstract:** ***The development of technology is certainly easier for a lot of good in terms of economy, education, culture and also raises much impact both positive effects and negative, a result of the negative impact that arise are the illegal contents which provide information such hatred of love, religion and race, how the shape of the crime whether it could include in a cyber crime or not, because there is no material or non-material losses from such actions.***

**Keyword:** Cyber Crime, Cyber Crime Perspective, Cyber Crime Indonesia, Development Technology, Illegal Information

## 1. Introduction

Utilization of information technology, media, and communications have changed the behavior of both human society and civilization globally, both directly and indirectly*[1]*[2][3].The development of information and communication technology has also led to the relationship become the world without borders and cause changes in the social, economic, cultural, and significantly progress is so fast even to the point that can not be avoided. Information Technology is currently a two-edged sword because while contributing to the welfare, progress, and human civilization, and effective means of tort unnoticed for some users actions unlawful *[1]*.

One of the technological developments that are often used and required all societies is a computer and smartphone. With a computer or smartphone one can easily use it for many things, but with the technology one can use it with good things or not, these actions included into Cyber crime where the crime is already unlawful in technology and someone who do can wear criminal law and civil*[2]*.

## 2. Theory

Computer-related crime or "cybercrime" or "e-crime" or "digital technology crime" is a long-established phenomenon, but the growth of global connectivity is inseparably tied to the development of contemporary cybercrime. Any criminal activity that involves a computer either as an instrument*[1][2]*,Cyber crime is a shape crime which uses the internet and the computer as a tool or a way to commit a crime. Problems associated with this type of crime eg hacking, copyright infringement, child pornography, child exploitation, carding and many crimes via the Internet. Also included breach of privacy when confidential information is lost or stolen, and others. In another definition, cybercrime is a term that refers to criminal activity with a computer or computer network into a tool, target or scene of the crime. Included into cybercrimes include online auction fraud, check forgery, credit card fraud, confidence fraud, identity fraud, child pornography, etc*[2]*.

The proliferation of digital technology and the convergence of computing and communication devices have transformed the way in which we socialise and do business. While overwhelmingly positive, there has also been a dark side to these developments. Crime follows opportunity; virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes. "Cybercrime" has been used to describe a wide range of offences, including offences against computer data and systems (such as "hacking"), computer-related forger and fraud (such as "phishing"), content offences (such as disseminating child pornography), and copyright offences (such as the dissemination of pirated content) *[2]*.

The magic of digital cameras and sharing photos on the Inernet is exploited by child pornographers. The convenience of electronic banking and online sales provides fertile ground for fraud*[1][3]*. Electronic communication such as email and SMS may be used to stalk and harass. The ease with which digital media may be shared has led to an explosion in copyright infringement. Our increasing dependence on computers and digital networks makes the technology itself a tempting target; either for the gaining of information or as a means of causing disruption and damage. The idea of a separate category of 'computer crime' arose at about the same time that computers became more mainstream*[2]*.

Generally speaking, computers play four roles in crimes: They serve as objects, subjects, tools, and symbols. Computers are the objects of crime when they are sabotaged or stolen. There are numerous cases of computers being shot, blown up, burned, beaten with blunt instruments, kicked, crushed and contaminated *[2]*. The damage may be intentional, as in the case of an irate taxpayer who shot a computer four times through the window of the local tax office; or unintentional, as in the case of a couple who engage in sexual intercourse while sitting on computer sabotage and destroy information, or at least make it unavailable. Computers play the role of subjects when they are the environment in which technologies commit crimes. Computer virus attacks fall into this category*[1][2]*. When automated crimes take place, computers will be the subjects of attacks. The third role of computers in crime is as tools, enabling criminals to produce false information or plan and control crimes. Finally, computers are also used as symbols to deceive victims. In a $50 million securities-investment

fraud case in Florida, a stock broker deceived his victims by falsely claiming that he possessed a giant computer and secret software to engage in high-profit arbitrage. In reality, the man had only a desktop computer that he used to print false investment statements. Hedeceivednew investors by paying false profits to early investors with money invested by the new ones *[2]* .

### A. Causes of Cyber Crime

Factors that affect cyber crime are:

1) Political factors. Observing the rise of cyber crime that occurred in Indonesia with the problems faced by enforcement, criminalization process that occurs in the field of cyber harm society. computer spread of the virus can destroy computer network used by the government, banks, businesses and individuals that might impact on the chaos in the system network. Can be ensured if the system is not functioning banking computer network in a single day would lead to chaos in banking transactions. This condition requires a policy of the Indonesian government to tackle cyber crime is growing in Indonesia. Law enforcement officials have been working hard to crack down on any of cybercriminals, but law enforcement can not afford to walk up to expectations of society because law governing special about cyber crime yet. To avoid greater losses due to the actions of cybercriminals will require government policies Indonesia to set up the special law (lex specialist) for cyber crime. With this law the law enforcement officers did not hesitate in enforcing the law against cyber crime.
2) Economic Factors. Economic progress of a nation is influenced by the sale of goods production. Computer networks and the Internet is a medium which is very cheap for sale. The world community many are using this medium to look for items individual and corporate interests. Goods produced by industries in Indonesia are many and loved by the international community. Business people should be able to utilize the internet facilities in question. The economic crisis that hit the Indonesian nation must be a lesson for the people of Indonesia to emerge from the crisis in question. All components of the Indonesian nation must participate in supporting the economic recovery. Internet media and computer networks is one medium that can be utilized by the whole society to promote Indonesia.
3) Socio-Cultural Factors. Socio-cultural factors can be seen from several aspects, namely:

a. Information technology advances. With information technology man can access environmental developments accurately, because that is where there is freedom that is balanced, even to actualize herself to be recognized by the environment.
b. Human Resources. Human resources in information technology has an important role as a controlling tool. Technology can be used for prosperity but also to acts that result in disastrous result of irregularities and abuse. In Indonesia Resources business information technology enough, however Resources to produce still lacking. This is due to the lack of research and lack of appreciation of the cost of research and study. So the Human Resources in Indonesia only be users only and is quite a lot.
c. New Community. With the technology as a means to achieve the goal, including the internet media as a vehicle to communicate, sociologically formed a new community in cyberspace.

### B. Types of Cyber Crime

The following are some types of cybercrime*[4]*:

1) Carding, is a crime to use computer technology to conduct transactions using credit cards so that others can harm the person is both material and non-material. in terms of online credit card fraud
2) Cracking, crimes using computer technology are being made to undermine the security system of a computer system and usually commit theft, anarchy so recording gain access. Usually we often misinterpret between a hacker and a cracker in which the hacker himself synonymous with negative actions, but hackers are people who love to program and believe that the information is something that is very precious and nothing can be published and confidential. Cracker being identical with a person who can change the characteristics and properties of a program that can be used and deployed at will
3) Joy computing, namely the use of another person's computer without permission
4) Hacking, ie accessing illegally or without authorization by means of a terminal
5) The Trojan horse, which is the manipulation of data or programs by changing the data or instructions in a program, delete, add, makes no coverage, with the aim of personal interests or others
6) Data leakage, which involves the leakage of data to the outside, especially regarding data that must be kept secret
7) Data diddling, is an act of changing data is valid or invalid lawful manner, change the input data or output data
8) To frustate data communication or a waste of computer data.
9) Illegal Contents, is a crime to enter the data or information to the internet about something that is UNTRUE, unethical, and may be unlawful or disturb public order. An example is the loading of a lie or slander will destroy the dignity or the dignity of others, matters related to pornography or loading an information is a state secret, agitation and propaganda against the legitimate government, and so on. Still remember Pritchard case mulyasarithe which until now has not been completed. Just because email writing slightly damaging the good name of a private health institution, he was dragged to court.

## 3. Related Work

There are few studies related to the cyber crime with a survey that has been done, here are some of the study authors feel pretty good on the presentation of data.

Folashade B. Okeshola *[4]*,This study shows the percentage is quite high crime rate in the country nigeria, crimes committed in cyberspace mostly a scam or spam emails and also pornography, based on a survey conducted randomly

with existing data The crime rate is accessing pornography and spamming.

Fawn T. Ngo and Raymond Paternoster *[5]*, This study used a sample of the data obtained from the students on the pattern of life that exist in everyday life, especially in accessing the Internet, based on the pattern that is then made visualization of internet abuse victims and what content is accessed and used for cyber crime

Dr. Abdullahi Y. Shehu*[6]*, Cyber-crime presents enormous challenges to society,especially developing societies that are trying to catch-up with the technology revolution, yet are relatively weaker to respond to the challenges of this development. The admittance of electronic evidence in court had untilrecently been a major obstacle to the successfulprosecution of fraud cases, not less so, those involving the misuse of hi-tech. The legal profession is not immune to the risks of cyber-crime and the challenges of preventing and prosecuting cyber criminals. There is no „one-fits-all" solution to this problem. Nonetheless, this paper identifies some remedies and priorities for action domestically, regionally and globally. The scope, prevalence, severity, and duration of cyber-crime and the need to identify high-risks among populations require systematic action.

Anah Bijik Hassan*[7]*, This research focuses on the societal conditions that exist in nigeria, For Nigeria to serve as a fertile ground for economic break through, it must be build on a crime free society. But an ideal economy is virtually not possible, because as technology increases so also crime rate. Cyber criminals will always keep in pace with any technological advancement. It is true that Technology gives rise to cyber crime. The future of our economy lies in our hands, the future itself is the summation of our decisions so we should believe in ourselves and endeavor to do the right thing at each point in time, following carefully the suggestions of this paper. Until then, the dreamed society will not become a reality.

## 4. Discussion

To maintain the security of the data when the data is sent and when the data has been stored on a computer network, then developed several techniques for data security. Some techniques for data security available today include:

a. Internet firewall is a computer network connected to the Internet needs to be provided with an Internet Firewall. Internet Firewall serves to prevent access from outside to the internal system. Thus the data are in the computer network can not be accessed by outsiders who are not responsible. Firewall works in 2 ways: using filters and proxies. Firewall filter to filter communications to occur as needed, only certain applications are allowed to pass and only a computer with a specific identity that could be related. Firewall proxy means allowing the user of the Internet To access the widest, but from the outside can only access a particular computer.
b. Cryptography is the art of encrypting data. The data will be sent disandikanterlebih before being sent over the internet. At the destination computer, the data is restored to its original form so that it can be read and understood by the recipient. Encoded data is so that if there are parties who intercepts the data transmission, the party can not understand the contents of the data sent because it is merely a password. Thus data security can be maintained. There are two processes that occur in cryptography, the encryption and decryption process. Encryption is the process of converting the original data into data passwords, while the decryption process is the process megembalikan password data into the original data. Aslin data or data to be encrypted is called plain text, while the encoding result data called cipher text. The encryption process occurs on the sender's computer before the data is sent, whereas decryption process occurs on the recipient's computer as soon as it is received so that the recipient can understand the data.
c. Secure Socket Layer (SSL) Line data transmission over the Internet through a lot of transitions and mastered by many people. This causes the data transmission over the Internet vulnerable to eavesdropping. Therefore, the browser is equipped with Secure Sockets Layer which serves to encode data. This way, the computers that are in between the sender and recipient computer can no longer read the contents of the data

Act No. 11 of 2008 on the Internet and Electronic Transactions (ITE) Law, which was passed and enacted on April 21, 2008, although to this day there has been no a Regulation concerning technical implementation, but is expected to be a cyber law or cyberlaw to ensnare cybercrime perpetrators were not held accountable and be a legal basis for the public users of information technology in order to achieve a legal certainty.

a. Article 27 of Law ITE 2008: Any person who intentionally and without right to distribute and / or transmitting and / or make the inaccessibility of electronic information and / or electronic documents that have a charge of violation of decency. Penalty of article 45 (1) Criminal Code. Imprisonment of 6 (six) years and / or a maximum fine of Rp 1,000,000,000.00 (one billion rupiah). Regulated in article 282 of the Criminal Code of crimes against decency.
b. Article 28 of Law ITE 2008: Any person who intentionally and without right of spreading false news and misleading consumers which resulted in losses in electronic transactions.
c. Article 29 of Law ITE 2008: Any person intentionally and without right transmit electronic information and / or electronic documents that contain the threat of force or scare for personally (Cyber Stalking). Penalty of article 45 (3) Any person who meets the elements referred to in Article 29 shall be punished with imprisonment of 12 (twelve) years and / or a maximum fine of Rp. 2,000,000,000.00 (two billion)
d. Article 30 UU ITE 2008, paragraph 3: Any person knowingly and without authority or unlawfully accessing computer and / or electronic system in any way to violate, break through, go beyond, or to break the security system (cracking, hacking, illegal access). Penalty of article 46, paragraph 3 every person who meets the elements referred to in Article 30, paragraph 3 shall be punished with imprisonment for a period of 8 (eight) and / or a fine of Rp 800,000,000.00 (eight hundred million rupiah).

e. Article 33 UU ITE 2008: Any person knowingly and without authority or unlawfully take any actions that result in disruption of the electronic system and / or cause the electronic system to not work as they should.
f. Article 34 of Law ITE 2008: Any person knowingly and without authority or unlawfully manufacture, sell, hold for use, import, distribute, provide or have.
g. Article 35 of the Law ITE 2008: Any person who intentionally and without right or unlawful manipulation, creation, alteration, removal, destruction of electronic information and / or electronic documents with the aim of electronic information and / or electronic documents such as if the data were authentic (Phishing scams website.

In Indonesia violation internet abuse cases is increasing every year following the total loss of the public's cyber crime cases in 2011 reached 4.8 billion in 2012 reached Rp 5, 2 billion and USD 56 448. "Whereas in 2013 reached Rp848 million," the police chief said while reminding the public to be careful in doing transactions online. below are the author will give a few examples of cases in Indonesia included in cyber crime.

These events have occurred in 2013, precisely on Thursday (03/14/2013). A student in Bandung entangled with the law for fraud in running his online business with a foreign exchange investment mode. This deception provides varied benefits package. Ranging from 50 percent, 70 percent, 100 percent, 300 percent. The more money invested by its clients, the greater the benefits, but a business run did not last long because there was a client report penipian them and the student charged under the Law on Information and ElectronicTransactions on penalty of six years and the Criminal Code of Fraud with a penalty of four years.

Another case is the police's official website was hacked in 2011, police investigating the perpetrators of hacking (hacking) official website is located at http://www.polri.go.id police, the police official Web page, until 17:00 pm May 16, 2011 difficult to access. Visitors are directed to the address http: //www.polri.go.id/backend/index.html containing images of two people raised the flag on the hill. Then came the black paper with the call for jihad.

Other cases are cases of gambling on the internet, Polda Metro Jaya to catch the perpetrators of online gambling road in front of the hospital Husada Great mango highway, West Jakarta. Police trace the origins of a site that was coming from outside the country.Director general regional police criminal detectives metro jaya, Sr. tony Herwanto, describes actors make use of the site as a media www.aseanbet.com gambling. Through these sites netted people to gamble actors in cyberspace by guessing the score of a ball game. The results of the gambling out every Tuesday and Thursday, if you win gambling revenue will go to a player's account and jka lost will go to the account of the perpetrator. Police are still chasing the existence of gambling site owners to track the internet protocol (IP) which was derived from overseas based on some of these cases, the use of information technology, media, and communications have changed the behavior of both human society and civilization globally. The development of information and communication technology (ICT) has also led to the relationship become the world without borders and cause changes in the social, economic, cultural, and significantly progress is so fast. Information Technology is currently a two-edged sword because while contributing to the welfare, progress, and human civilization, and effective means against the law. When this has been born a new legal regime known cyber law or telecommunications law. Cyber law, internationally used term for the law relating to the use of (ICT). Similarly, telecommunications law which is a manifestation of the convergence of telecommunications law, media law, and legal informatics.

Other terms are also used information technology law, the law of cyberspace. The term birth because the activities carried out through a network of computer systems and communication systems both locally and globally by utilizing information technology-based computer system is an electronic system that can be viewed virtually. Legal issues often encountered is when associated with the delivery of information, communication and / or electronic transactions, especially in terms of evidence and matters related to legal actions carried out through the electronic system.

## 5. Conclusion

Cybercrime is one of the forms of crime that should be avoided or eradicated well being. Cyberlaw is one of the tools used by a country to fight and control cybercrime (cybercrime) particularly in the case of cybercrime is growing in the country's territory. Like lawbreakers and law enforcement, enforcement cyberlaw can be done with the establishment of clear rules that state that does not conflict with existing laws.

## References

[1] E. Casey, Digital Evidence and Computer Crime, USA: Elsevier, 2011.
[2] M. Chawki, A. Darwish, M. A. Khan dan S. Tyagi, Cybercrime, Digital Forensics and Jurisdiction, New York: Springer, 2015.
[3] J. Sammons, Digital Forensics Threatscape and Best Practices, USA: Elsevier, 2016.
[4] A. K. Adeta dan F. B.Okeshola, “The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria - Kaduna State, Nigeria,” American International Journal of Contemporary Research, vol. III, no. 9, pp. 98-101, 2013.
[5] F. T. Ngo dan R. Paternoster, “Cybercrime Victimization: An examination of Individual and Situational level factors,” International Journal of Cyber Criminology, vol. V, no. 1, pp. 773-793, 2011.
[6] Dr. Abdullahi Y. Shehu , “Emerging Issues in Cyber-Crime: Causes, Implications and Effects for the Legal Profession,” Online Journal of Social Sciences Research, vol. III, no. 7, pp. 169-180, 2014.
[7] A. B. Hasan, F. D. Lass dan J. Makinde, “Cybercrime in Nigeria: Causes, Effects and the Way Out,” ARPN Journal of Science and Technology , vol. II, no. 7, pp. 626-631, 2012.