Asian Journal of Applied Science and Technology (AJAST)
Volume 1, Issue 8, Pages 122-124, September 2017

Cybercrime: An Analysis from Positive Law Perspective

Ibnu Wihansyah

Master Degree in Communication Science Department, Sebelas Maret University, Indonesia. Email: ibnuwihansyah@gmail.com

Article Received: 05 August 2017 *Article Accepted: 19 September 2017* *Article Published: 24 September 2017*

ABSTRACT

Technology development is a necessity. Information and Communication Technology is a large dome of terminology that includes all technical equipment for processing and conveying information. It has also caused the world's relationships to be unconstrained. It's here and now means it's somewhere else and now. In every line of technological life present that contributes its role to the desired coveted will be better. That dream is in fact two blades facing each other. In the body of one knife exactly each other. On the one hand technology contributes to the improvement of welfare, progress, and human civilization. Furthermore, on the other hand, technology can be an instrument in the act against the law. With human information technology then likes getting a vehicle to burst its criminal lust. Criminal crime by taking technology as a medium, then manifested in various forms. These forms include hacking, cracking, and so on. Do not be surprised if for example your balance arrives – suddenly reduced, or the bank hundreds of millions in the automatic teller machines suddenly disappeared. Technology is the last human love, so no wonder humanity is often subject to that technology.

Keywords: Information Technology, Cybercrime and Positive Law.

1. INTRODUCTION

Human need for internet technology is increasing. Apart from being a medium of information providers, through internet also commercial community activities become the largest and rapid growth and penetrate the various borders of the country. Even through this network market activity in the world can be known for 24 hours. Via the internet or also called *cyber space*, anything can be done. The positive aspect of this virtual world of course adds technology development *trend* of the world with all forms of human creativity. But the negative impact cannot be avoided. When pornography rampant in the internet media, the community cannot do much. along with development of Internet technology, leading to the emergence of so-called *cybercrime* crimes or crimes through the Internet. The emergence of several cases of *cybercrime* in Indonesia, such as credit card theft, *hacking* some sites, intercepting other people's data transmission, such as e-mail and manipulate data in ways unintended prepare orders into computer *programmer.* So in the crime of the computer is possible the offense formal and material offense. Formal crime is the act of someone who enters someone else's computer without permission, while material offense is an act that causes harm to others. *Cybercrime* has become a threat their stability, so the government is difficult to compensate for the crimes committed techniques with computer technology, especially the Internet and intranet. This paper will discuss how to identify, understand and know all the *online* activities of daily living *(cyber)* which has a risk of crime *(crime)* to be anticipated in order to avoid loss of both material and non-material. This analysis aims to provide information that has been summarized from the many forms of crime that exist in cyberspace. Know all forms of crime risk in cyberspace so that bias is anticipated before the loss occurs.

2. BASIC THEORY

Cybercrime born from *hacking* activity that has been there more than a century. In the 1870s, some teenagers have damaged the country's new telephone system by changing authority. The following will show how busy the hackers have been there for 35 years. As early as 1960 the university facilities with the main frame of a large computer, such as artificial intelligence laboratory *(artificial intelligence)* MIT, became an experimental stage for *hackers.* At first, the word *"hacker"* means a positive to a master computer that can create a program beyond what it was designed to do its job.

Early 1970 John Draper made a phone call making a long distance phone call for free by blowing the right tone into the phone telling the phone system to open the channel. Draper finds a whistle as a free gift in a box of children's cereals. Draper, who later gained the nickname *"Captain Crunch"* was arrested repeatedly for the destruction of the telephone in 1970. *Yippie* start a *social* movement YIPL magazine / TAP *(Youth International Party Line / Technical Assistance Program)* to help the *hackers* phone (called "phreaks") make long distance calls for free. Two members of California's Homebrew Computer Club begin making *"blue boxes"* tool used to hack into phone systems. Its members, who adopted the handle *"Blue Berkeley"* (Steve Jobs) and "Oak Toebark" (Steve Wozniak), who later founded Apple Computer. Author William Gibson early 1980 includes the term *"Cyber Space"* in a science fiction novel called *Neurimancer*. In the first arrests of *hackers,* the FBI raided the headquarters of 414 in Milwaukee (named after the local area code) after members cause a computer break-ins 60 of the memorial Sloan-Kettering Cancer Center to Los Alamos National Laboratory. *Comprehensive Crime Control Act* gives *Secret Service* jurisdiction over credit cards and fraud Komputer.dua hackier form groups, *the legion of doom* in the United States and *the Chaos Computer Club* in Germany.

Late 1980 of computer fraud and other abuses of members more power to the federal authority *computer emergency response team* formed by defense agencies the United States based on the Carnegie Mellon University in Pittsburgh, its

mission to investigate the development of the volume of attacks on computer networks at the age of 25, a a veteran hacker named Kevin Mitnick secretly monitors emails from MCI and a digital security equipment employee. he was convicted of damaging computers and steal *software* and it is declared legal for one year in prison. In October 2008 appeared something new virus called *Conficker* (also called *Down up Down up* and *Kido)* that terkatagori as worm type virus. Conficker attacks Windows and is mostly encountered in windows XP. Microsoft released *a patch* to stop this worm on 15 October 2008. Heinz Haise estimate *Conficker* has infected 2.5 million PCs 15 January 2009, while the *guardian* estimated that a 3.5 million PCs infected. On January 16, 2009, this worm has infected nearly 9 million PCs, making it one of the fastest infections spread in a short time. Cybercrime is a benthic of crimes arising out of the utilization of internet technologies assumes some opinion *cybercrime* with computer crime. The US Department of Justice provide an understanding of computer crime as *"any illegal act requiring knowledge of computer technology for its perpetration, and investigation* ". The definition identical to that given the Organization of the European community development, which defines computer crime as *"any illegal, unethical or unauthorized behavior Relating to the automatic processing and / or the transmission of data".* Andi Hamzah (1989) in his "criminal aspects in the field of computer" defines computer crime as "Crime in the computer field can generally be defined as the use of illegal computer". From some of the above, in summary it can be said that *cybercrime* can be defined as the unlawful act committed by using the Internet based on the sophistication of technology, computers and telecommunications both for profit or not, to the detriment of the other party.

3. DISCUSSION

3.1. Typology of Cybercrime

So far in conventional crime, there are two types of crimes: (a). Blue Collar Crime and (b) White Collar Crime. The blue-collar crime is often understood to be criminal or non-criminal based on conventional action. Conventional criminal acts such as theft, rape, murder, robbery and so forth. Whilst white-collar crime is understood as a more specific mode of crime, the outline of this type of crime is divided into four crime groups: corporate crime, bureaucratic crime, malpractice, and individual crime. Cybercrime itself as a crime that emerged as a result of the virtual world community on the internet, has its own characteristics that are different from the two models above. The unique characteristics of these cybercrimes include the following: (1) The scope of the crime, (2) The nature of the crime, (3) The offender (4). Crime mode and (5). The types of losses incurred. From some of the above characteristics, to facilitate handling of the cybercrime can be classified into: (a). Cyberpiracy. The use of computer technology to reprint software or information, and then distribute the information or software via computer technology. (B). Cybertrespass. Use of computer technology to improve access to an organization's computer system or individual (c). Cybervandalism. The use of computer technology to create programs that disrupt the electronic transmission process, and destroy data computing.

In this context, the issue of the type of cybercrime will be considered by the motive can be divided in several ways: (1) Cybercrime as an act of pure evil. At this level, cybercrime is understood as a crime in which a person committing a crime is committed intentionally. So there is a very strong element on the nature of deliberate and planned action to do so. Form of action is vandalism, theft, and anarchy, against an information system network or computer system. (2). Cybercrime as a gray crime. The modus operandi of this model crime is actually confusing to be categorized as a crime or not. This crime is not clear between a criminal offense or not because he committed a burglary to a system but did not vandalize, steal or commit anarchist deeds. So the conditions that occur in this case as safe does not happen something to the information system or computer system.

Furthermore, (3). Cybercrime attack individuals. This model's crime is committed against others with a vengeful or idle motive, with the aim of damaging a person's good name, trying or finishing someone to gain personal satisfaction. The measure is personal satisfaction with the subject being obsessed. Examples of cybercrime are pornography, cyberstalking, etc. (4). Cybercrime attack the copyright (property rights). Crimes committed on the work of someone with a motive to double, marketing, change aimed at personal interest / public nor by the material and non-material. (5). Cybercrime attack the government. Crimes committed by the government as objects with the motive of terror, pirating or destructive security of a government that aims to disrupt the system of government, or destroy the State.

3.2 Modus Operandi of Cybercrime

The modus operandi of cybercrime consist as: (1). Unauthorized Access to Computer System and Service. Crime committed by entering / infiltrated into a computer network system illegally, without permission or without the knowledge of the owner of the computer network system he entered. Usually the perpetrators (hackers) do so with the intention of sabotage or theft of important and confidential information. However, there are also those who do just because they feel challenged to try their skills through a system that has a high degree of protection. This crime is increasingly prevalent with the development of internet / intranet technology. (2). Illegal Contents. It is a crime to enter data or information to the internet about something that is untrue, unethical, and may be considered unlawful or disturbing public order. For example is the loading of a false or slanderous report that will destroy the dignity or self-esteem of others, matters relating to pornography or the loading of information which is state secret, agitation and propaganda against the legitimate government, and so on. (3) Data Forgery. It is a crime to forge data on important documents stored as scriptless documents over the internet. Crime is usually directed at the documents in e-commerce by making as if it happened "typo" that will eventually profitable actors. (4) .Cyber Espionage. A crime that utilizing the Internet to conduct espionage against other parties, by entering into the computer network system (computer network system) the target. This crime is usually directed against business rivals whose documents or data of importance are stored in a computerized system. (5). Cyber

Sabotage and Extortion. This crime is committed by making interference, destruction or destruction of a data, computer program or computer network system connected to the internet. This crime is usually done by inserting a logic bomb, computer virus or a particular program, so that the data, computer programs or computer network system can not be used, is not working properly, or run as desired by the perpetrator. In some cases after it occurs, the offender offers to the victim to repair the data, computer program or computer network system that has been sabotaged, of course with a certain fee. These crimes are often referred to as cyberterrorism. (6). Offense against Intellectual Property. This crime is directed against Intellectual Property Rights owned by others on the internet. An example is the impersonation of the display on the web page of another person's site illegally, broadcasting an information on the internet that turns out to be someone else's trade secret, and so on. (7). Infringements of Privacy. This crime is directed against personally identifiable information. These crimes are usually directed against the private information a person stored in the form of personal data stored in computerized, which if known by others it can be victims of harmful material or immaterial, such as credit card number, ATM PIN number, disability or illness hidden and so on. (8). Cracking. Crime by using computer technology is done to damage the system of the security of a computer system and usually do the theft, anarchist action so that gaining access. Usually we often misinterpret between a hacker and a cracker in which the hacker himself identetik with negative actions, but hackers are people who love to program and believe that the information is something that is very precious, and nothing is to be published and confidential. (9). Carding. It is a crime by using computer technology to conduct transactions using another person's credit card so that it can harm the person either material or non material.

4. End Of Discussion

To cope with the increasingly widespread Internet crime it requires an awareness of each country will the dangers of internet abuse. then the following is the step or way of handling globally: (1). The modernization of national criminal law along with its procedural law is harmonized with international conventions relating to such crimes. (2). Increased security standards nationwide computer network system in accordance with international standards. (3) To improve the understanding and expertise of law enforcement agencies regarding prevention, inventigasi, and prosecution of cases that relate to cybercrime. (4). Increase citizen awareness about the dangers of cybercrime and the importance of crime prevention . (5) Enhance cooperation among States in the field of technology regarding cybercrime law violations. Enforcement of cybercrime especially in Indonesia is influenced by five factors: the Law, the mentality of law enforcement officers, community behavior, infrastructure and culture. The law can not be upright by itself always involves human in it and also involves human behavior in it. The law also can not erect by itself without the existence of law enforcers. Law enforcement is not only required for professionals and smart in applying legal norms but also dealing with someone and even a group of people suspected of committing a crime. With seiringnya the times and the development of the world of crime, in particular the development of cybercrime is increasingly worrisome, law enforcement agencies are required to work hard for law enforcement become the main subject of the fight against cybercrime. For example, UN Resolution No.5 of 1963 on efforts to combat the misuse of Information Technology on December 4, 2001, gives an indication that there is a serious international problem, serious and must be addressed. The Code of Penal (Penal Code) is still used as the legal basis for capturing cybercrime, in particular the type of cybercrime that meets the elements in the articles of the Criminal Code. Some of the legal grounds in the Criminal Code used by law enforcement officers include: (1). Article 167 of the Criminal Code, (2). Article 406 paragraph (1) of the Criminal Code, (3). Article 282 of the Criminal Code, (4). Article 378 of the Criminal Code (5) Article 112 of the Criminal Code, (6) of Article 362 of the Criminal Code, (7) of Article 372 of the Criminal Code. In addition to the Criminal Code, there are Laws related to this matter, namely Law No. 11 of 2008 on Information and Electronic Transactions (EIT Law), where the rules of crime that occurred therein proved to threaten the internet users. Since the enactment of Law No. 11 Year 2008 on Information and Electronic Transactions on 21 April 2008, has caused many victims. Based on the monitoring that has been done by the author at least there are 4 people who called the police and became a suspect for allegedly committing a crime stipulated in the Law on EIT. The suspects or victims of the EIT Act are active internet users who are accused of insulting or related to the contempt content on the internet. (attached data) People who are charged under the EIT Law will all be exposed to the possibility of article 27 paragraph (3) in conjunction with Article 45 paragraph (1) of the Act EIT namely the threat of 6 years in prison and a fine of 1 billion rupiah. EIT Law can be used to beat all activities on the internet without exception journalists or not. Because the formula is very flexible.

References

[1] Barda Nawawi, Arief (2005) Renewal of Criminal Law In Perspective of Comparative Study, Bandung: Citra Aditya.

[2] (2006) Criminal Act Development of Cybercrime Study in Indonesia, Jakarta: Raja Grafindo Persada.

[3] Mahayana, Dimitri, (2000). Picking Future, Futuristic and Community Engineering Towards a Global Era, Rosda, Bandung.

[4] John Nasibitt, Nana Naisbitt and Douglas Philips, (2001). High Tech, High Touch, Search Meaning in the Middle of Rapid Development of Technology, Mizan, Bandung.

[5] Sudarto (1986). Law and Criminal Law, Bandung: Alumni.

[6] Wiener, N. (1948), Cybernetics: or Control and Communication in the Animal and the Machine, New York: Technology Press / John Wiley & Sons.