INTERNATIONAL JOURNAL OF SOCIOLOGY, POLICY AND LAW (IJOSPL)
Vol.2 No.3 June 2021 E-ISSN : 2774-2245

CYBER CRIME IN A CRIMINOLOGY PERSPECTIVE

Anshori

Faculty of Law, University of Billfath Lamongan
Indonesia
anshori@billfath.ac.id

Abstract *— The reason for choosing this research, started from the phenomenon of crime which is integrated with the development of information technology. The discussion in this study uses the concept method. The function of theory in this study is to examine the phenomenon of crime that has developed its relevance to the development of information technology. Cyber crime is an unlawful act / virtual crime (not real) that utilizes computer media connected to the internet and exploits other computers connected to the internet. Theory serves as a tool to simplify and understand a problem. In this context, several criminological theories can be used to understand the perpetrators and modes of cyber crime, so that a complete picture of cyber crime and its perpetrators is obtained. There are four theories that can be used to analyze cyber crime, namely anomie, differential association, social control and neutralization.*

Keywords— *Put Crime , Cyber World , Criminology Perspective.*

I. INTRODUCTION

The development of the times and rapid technological advances have a major influence on socio-cultural changes, one of which is regarding the phenomenon of crime and its transformation. The phenomenon of crime is an eternal problem in human life, because crime develops in line with the development of the level of human civilization.

Crime as a phenomenon is born and is the impact of several factors such as economy, association, existing opportunities and others. These factors that occurred in Indonesia have shown a negative effect. The large number of people who commit acts that are classified as crimes, solely to meet their needs.

Demanding a critical study to find out the cause of a person committing a crime, this can be done using criminological theories. Although abstract, this theory is needed to examine why there are humans who are able to implement social norms and legal norms, but there are also humans who actually violate them. These theories are not only important for academic and research activities, but also important for the education of citizens.

Along with the rapid development of telecommunications technology and computerized technology, the internet is multifunctional. This development brings us to the threshold of the fourth revolution in the history of human thought, when viewed from the construction of human knowledge which is characterized by a borderless way of thinking . The acceleration of technology is getting more and more supra which also has a negative impact, one of the causes of changes in multidimensional crime as well.

From the analysis of the review above, a crime term appears which is commonly called "Cyber Crime". The existence of Cyber Crime has become a threat to stability, so that the government is difficult to balance the techniques of crimes committed with computer technology, especially internet and intranet networks. This is a result of the rapid development of information technology, so that every development essentially brings the effect of two sides of a coin, each of which is interrelated and will not be separated, in the form of a positive side and a negative side. Perpetrators as well as victims of crime are generally human.

The author believes that there are many criminological theories that can be used to understand cyber crime in this paper, the author only reviews some criminological theories to be used to study cyber crime. This is based on the consideration that theoretically there is a match between the propositions in these theories and the characteristics of crime, the characteristics of criminals, and public reactions to cyber crime in Indonesia. The results of this study can be used as one of the considerations for planning criminal policy measures against cyber crime in Indonesia, especially in penalization and non-penal policies.

II. LITERATURE REVIEW

Anomie Theory

Anomie theory was put forward by the French sociologist, Emille Durkheim (1858-1917), and Robert K. Merton . Durkheim's opinion was put forward before Merton's . Durkheim use the term anomie to refer to a

condition that is deregulated. According to him, the rapid and gripping social changes in society have a major influence on all groups in society. The main values and values that have been accepted by the community become blurred and even disappear. This situation encourages the occurrence of norm uncertainty and even the absence of norms . Durkheim describes the concept of anomie as a condition in society where there is hopelessness or the absence of norms. Anomie is also the result of rapid societal change.

Anomie exists in every society and manifests not only in the form of crime but also in cases of suicide. All this happens because of the absence of social norms, and the absence of social control that can control deviant behavior. Furthermore, Durkheim explained that, the state of deregulation is defined as a condition of not obeying the rules that exist in society, and members of society do not know about what is expected by others. This situation is considered as the cause of deviant behavior. Based on the studies conducted, Durkheim stated that the average suicide rate in society is the final act of an anomie condition which is rooted in two conditions, namely Social integration and Social regulation . Furthermore, it is explained that suicide is caused by 3 conditions, namely deregulation of needs or anomie, outrageous regulation or fatalism, and lack of structural integration or egoism.

Robert Merton further revealed that deviant behavior is considered an abnormal behavior because the behavior originates in the individual. Deviant behavior arises because there are a number of people who feel the gap between the goals they have (goals) and the available means to achieve these goals. In every society there are two types of social norms , namely social goals (social goals) and available means (acceptable means) . Ideally in every society there are goals to be achieved and there are legitimate means to achieve them. In practice, not everyone can use the available means to achieve goals. Therefore, many people impose their will to achieve their goals, even though the methods used violate the law (illegitimate means). This way of achieving a goal that violates the law is called crime.

Differential Association Theory

Differential Association Theory was proposed by an American sociologist, Edwin H. Sutherland in 1939 which was later refined in 1947. This theory was built based on 3 theories, namely Ecological and Cultural Transmission Theory of Shaw and McKay; Symbolic Interactionism by George Mead; and Culture Conflict Theory.

Romli Atmasasmita stated that systematic understanding is career crime or organized practices of crime. The definition of organized practice of crime is behavior that supports the norms that have developed in society. In 1947, Sutherland replaced the term "Social disorganization" with "Differential social organization". Through the replacement of the term, Sutherland wants to show the existence of various social conditions with internal values and goals. Application of Criminological Theories in Crime Prevention each to be used as a different means in achieving the goal. This theory recognizes the existence of various social organizations that are separate, but compete with each other based on their own norms and values.

Based on the proposition above, Sutherland emphatically refutes Cesare Lombrosso's theory, which states that evil behavior is brought by a person from birth (evil human). According to Sutherland, bad behavior can be learned from others through the process of interaction and communication. Sutherland 's opinion gets support from Glaser who states that crime is not only learned through direct interactions between individuals, but can also be learned even though the individuals do not meet, and the mass media becomes the intermediary.

Social Control Theory

Social Control Control theory is a classification of theories that claim not to ask why people commit crimes, but why they do not commit crimes? These theories assume that everyone has a desire to commit criminal and deviant acts, and seek to answer why some people refrain from doing so.

In relation to control theory, according to Reiss, there are 3 components that can explain juvenile delinquency, namely the lack of reasonable internal control during childhood, the loss of control, and the absence of social norms or conflicts between these norms (at school, at school, in the community). family, or neighborhood). Furthermore, Reiss distinguishes 2 types of control, namely:

1. personal control , namely the ability of a person to refrain from achieving his goals in a way that violates norms;
2. social control , namely the ability of the community or social group to implement norms or laws and regulations.

Reiss concludes that the weakening of social control also results in deviant behavior. Proponents of control theory apparently agree that delinquency is the result of something lacking, namely a reduction in some of the bonds and control forces in society.

Neutralization Theory

The main opinion of the neutralization theory (neutralization on theory), that someone will learn to neutralize the morals that control human behavior, then commit deviant behavior. In addition, this theory explains how youths commit deviance, and how these youths engage in deviant behavior. David Matza confirmed. Neutralization theory emphasizes the learning process of young people to rationalize deviant behavior that is

carried out so that it is expected to deceive the work of social values and norms in society. John Hagan puts it this way.

Neutralization theory assumes that human behavior is controlled by the thoughts of the perpetrator. This theory asks , what is behind the thoughts of good people that sometimes make them turn into people who behave badly or badly or deviate from societal norms? Based on these questions, this theory assumes that most people, most of the time, when doing something actions are controlled by good thoughts, but why do people who generally have good thoughts do deviant actions or commit crimes.

Furthermore, Sykes and Matza describe 5 (five) neutralization techniques that can be carried out by criminals, which are as follows:

1. Denial of Responsibility , where the perpetrator describes himself as people who are powerless in the face of societal pressures (for example, lack of love from parents, being in a bad association or environment).
2. Denial of Injury , i.e. the perpetrator holds the view that the act committed does not cause great harm to the community.
3. Denial of Victim , namely the perpetrator understands himself as "the avenger", while the victims of his actions are considered guilty.
4. Condemnation of the Condemners , namely the perpetrators assume that people who condemn the actions that have been committed are hypocrites, hypocrites, as perpetrators of hidden crimes, out of envy, and so on.
5. Appeal to Higher Loyalities , namely the perpetrator feels that he is trapped between the will of the community and the legal provisions that exist in society with the needs of a smaller group, namely the group where they belong or join. Based on the explanation of the neutralization theory above, it can be understood that the neutralization theory reveals that deviant or evil behavior is carried out by a person because it is based on his own thoughts and is driven by several conditions outside the individual, so that the per

III. METHOD

Approach

empirical normative approach. The normative approach is used because it is used to research or describe and explain legal rules or norms that review crime in the perspective of concepts and theories that explain the factors that occur in crime.

To answer the legal problems in this legal research, several approaches to the problem will be used as follows:

a. Approach to legislation (statute approach);
b. Conceptual approach (conceptual approach);
c. Case approach (case approach)

The statutory approach is an approach that is carried out by examining all laws and regulations that are related to the problems (legal issues) that are being faced. For example, this statutory approach is carried out by studying the consistency/compatibility between the Constitution and the Law, or between one law and another, and so on .

Conceptual approach (conceptual approach) is a type of approach in legal research that provides an analytical point of view of problem solving in legal research seen from the aspects of the legal concepts that lie behind it, or even can be seen from the values contained in the norming of a regulation in relation to the concepts of law. concept used. Most of this type of approach is used to understand the concepts related to normalization in a legislation whether it is in accordance with the spirit contained in the underlying legal concepts. This approach departs from the views and doctrines that develop in the science of law.

This approach is important because understanding the views/doctrines that develop in legal science can be a basis for building legal arguments when solving legal issues at hand. The views or doctrines will clarify ideas by providing legal understandings, legal concepts, and legal principles that are relevant to the problem.

IV.RESULT AND DISCUSSION

Definition and Types of Cyber Crime (Cyber Crime)

The mother of cyber crime is cyber space , where cyber space is seen as a world of computer-based communication. In this case, cyber space is considered as a new reality in human life which in everyday language is known as the internet. This new reality is in fact formed through a computer network that connects between countries or between continents based on protocols. This means that in its working system it can be said that cyber space has changed distance and time to be unlimited.

However, advances in information technology (internet) and all forms of benefits in it bring their own negative consequences where it is easier for criminals to carry out their actions which are increasingly troubling the community, the abuse that occurs in cyber space is then known as cyber crime or in other literature the term is used. computer crime .

Cyber crime is an unlawful act / virtual crime (not real) that utilizes computer media connected to the internet and exploits other computers connected to the internet. The unique characteristics of cybercrime include, among others , five things:

a) Scope of crime
b) The nature of crime
c) Crime mode
d) Perpetrator
e) Losses caused

1. Scope of Crime

So far, in conventional crime, there are two types of crime, namely:

a. Blue collar crime or blue color crime This crime is a crime that is done conventionally such as robbery, theft, murder.
b. White-collar crime or white color crime This crime is a crime committed in groups or in an organized manner. These crimes are divided into four groups, namely corporate crimes, bureaucratic crimes, malpractice, and individual crimes. Cyber crime itself is a crime that arises due to the existence of a virtual world community on the internet. This pattern of crime is a "grey" area

Nature of Evil

The nature of cyber crime can be classified as follows:

a. Cyber crime as a criminal act Cyber crime as a criminal act is a crime committed with a criminal motive that uses the internet as a means of crime such as theft of ATM pin numbers and carding, namely the theft of credit card numbers belonging to others to be used in trade transactions on the internet; and the use of internet media (webserver, mailing list) to distribute pirated materials. Anonymous e-mail senders that contain promotions (spamming) can also be included in examples of crimes that use the internet as a means. In some developed countries, spammers can be prosecuted for breach of privacy.
b. Cyber crime as a "gray" crime Types of crime on the internet fall into the "gray" area. Therefore, it is difficult to determine whether this act is a criminal act or not considering that the motive for the activity is sometimes not for a crime. One of the examples is probing or port-scanning. This is the term for the act of spying on someone else's system by gathering as much information as possible from the system to be misused.

Crime Mode

Based on the mode of internet crime, crimes that are closely related to the use of computer-based technology and telecommunications networks are grouped into several forms, including:

a. Unauthorized Access to Computer System and Service This crime occurs when someone infiltrates a computer network system belonging to another person illegally, without permission, or without the knowledge of the owner of the computer network system that he/she enters. Probing and port are examples of this crime.
b. Illegal Contents Crime by entering data or information into the internet about something that is not true, unethical, and can be considered unlawful or disturbing public order. One example of this crime is loading false news or slander that destroys the dignity or self-esteem of other parties , matters related to pornography, or contains information that is a state secret.
c. Data Forgery This crime was carried out with the aim of falsifying data on important documents on the internet. These documents are usually owned by institutions or institutions that have web-based database sites.
d. Cyber Espionage, Sabotage, and Extortion Crimes that use the internet to spy on other parties. This crime is committed by entering the target party's computer network system. Sabotage and extortion are types of crimes committed by disrupting or destroying data, computer programs, or computer network systems connected to the internet.
e. Data Theft A crime that illegally takes computer data belonging to another person, either for their own use or for the use of others. Identity theft is one of the crimes followed by fraud.
f. Infringements of Privacy This crime is usually directed at someone's personal information on a computerized form of personal data stored. If known to others , this data can harm the victim materially or immaterially, such as credit card numbers, ATM PIN numbers.
g. Cyber Terrorism Cyber terrorism is an act of cyber crime that threatens the government or citizens, including cracking into government or military sites. For example, the case of Ramzi Yousef, the mastermind behind the first attack on the WTC building. Ramzi is known to store uniform details in encrypted files on his laptop.

Perpetrator

Criminals in cyber crime are called hackers and crackers. Examples of actions carried out by hackers and crackers include:

a. theft and use of other people's internet accounts
b. modification is known as defacement.
c. piracy can be done by exploiting security holes. One of the steps that crackers take before entering the targeted server is to do reconnaissance. The way to do this is by doing ports scanning or probing to see what services are available on the target server. Sample scanning results can show that the target server is running the Apache web server program, Sendmail mail server, and so on.
d. spread of viruses to computers. The spread is done using e-mail, often people whose e-mail system is exposed to viruses are not aware of it. This virus is sent elsewhere via his e-mail. There are quite a few cases of this virus, such as the Mellisa virus, I Love You, and SirCam.
e. DoS attack is an attack that aims to paralyze the target (hang, crash) so that it cannot provide services. This attack does not carry out theft, eavesdropping, or falsification of data, but with the loss of service, the target cannot provide services so there is a financial loss.
f. Domain name related crimes . Domain names are used to identify companies and trademarks. Many people try to make a profit by registering the domain name of someone else's company and then trying to sell it at a higher price. The term is often used is cybersquatting.

The targets of cyber crimes can be grouped into the following categories:

a. Cyber crime that attacks individuals (Against Person) The target of this type of crime is aimed at individuals or individuals who have certain characteristics or criteria according to the purpose of the attack. One example of this crime is pornography, which is an activity carried out by making, posting, distributing, and spreading pornographic, obscene and exposing material that is inappropriate (Hinea, 2005).
b. Cyberstalking Activities carried out to annoy or harass someone by using a computer, for example by using e-mail that is carried out repeatedly as well as terror in the cyber world. These disorders can be sexual, religious, and others.
c. Cyber-Tresspass Activities that violate other people's privacy areas such as web hacking, breaking into PCs, probing, port scanning.
d. Cyber crime attacks property rights (Against Property) Cyber crime is carried out to interfere with or attack the property rights of others. Some examples of this type of crime include unauthorized computer access through cyberspace, illegal possession of electronic information/information theft, carding, cybersquating, hijacking, data forgery and all activities that are detrimental to the property rights of others.
e. Cyber crime against the government (Against Government) Cyber crime Against Government is carried out with the specific purpose of attacking the government. Such activities include cyber terrorism as an act that threatens the government, including cracking on official government websites or military sites.

Loss Type

a term given to people who commit internet crimes whose impact is detrimental to internet service users. The victims think that the cracker is a criminal. The impact of losses caused by the cracker is material and non-material. Examples of Cyber Crime in the Indonesian Legal System 39 material losses are the misuse of ATM pin numbers, credit cards, and others. Examples of non-material harm are pornography, defamation , and others.

2 Criminological Theories to Study Cyber Crime (Cyber Crime)

The existence of crime, whether conventional or unconventional, is not something that stands alone, meaning that crime is the causality of several variables that surround a person so that that person commits a crime. Criminological theories further emphasize that crime is not an act born from a vacuum. Along with the emergence of information technology, crime has a new meaning. The visible room, as a place (locus) in committing crimes. This cyber crime emerged along with the rapid development of information technology. According to the British Police, cyber crime is all kinds of use of computer networks for criminal and/or high-tech criminal purposes by abusing the convenience of digital technology .

Meanwhile, according to Peter, Cyber crime is " The easy definition of cyber crime is crimes directed at a computer or a computer system. The nature of cyber crime, however, is far more complex. As we will see later, cyber crime can take the form of simple snooping into a computer system for which we have no authorization. It can be the feeing of a computer virus into the wild. It may be malicious vandalism by a disgruntled employee. Or it may be theft of data, money, or sensitive information using a computer system ." Another definition of cyber crime is a type of crime related to the use of unlimited information technology and has strong characteristics with an engineering technology that relies on a high level of security and credibility of information submitted and accessed by internet customers .

In two United Nations Congress documents quoted by Barda Nawawi Arief, regarding The Prevention of Crime and the Treatment of Offenders in Havana Cuba in 1990 and in Vienna Austria in 2000, he explains that there are two terms related to the definition of Cyber crime , namely cyber crime . and computer related crimes . In the background paper for the UN Congress X/2000 workshop in Vienna Austria, the term cyber crime is divided into two categories. First, cyber crime in a narrow sense is called computer crime . Second, cyber crime in a broad sense is called computer related crime . Complete as follows:

a. Cyber crime in a narrow sense (computer crime): any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed byh them.
b. Cyber crime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network.

From the explanation of cyber crime above, in the perspective of criminology, it is not the media of crime as the focus, any type of crime with very varied media, including crimes with computers as the instrument, it is certain that there are factors that trigger the crime. The easy use of technology without strong social control is a stimulus for committing crimes, and computer-based crimes are crimes that are accompanied by certain skills, without knowing the ins and outs of computers, it is impossible to use computers as a medium in crime.

The loose control of cyber crime, because there is no penal or non-penal policy that is expressly in the context of overcoming cyber crime, this is in accordance with the opinion of Muladi and Barda Nawawi Arief regarding law enforcement in order to be effective it must go through criminal law politics (criminal policy). or rational criminal law policies. The rational enforcement of criminal law consists of three stages, namely the formulation stage (legislative policy stage), application stage (judicial policy stage) and execution stage (administrative policy stage). Criminal policy is one way or alternative in solving crime problems because basically legal politics is essentially a policy from the state through authorized bodies to establish the desired regulations that are expected to be used to express what is contained in society and to achieve goals. what he aspires to.

Cyber crime with its various forms and modes is the end result of several factors that influence it, social aspects and the legal system as an instrument of control against criminals are enough to give color to cyber-based crimes. With a variety of criminological theories, it is quite helpful in photographing the occurrence of crimes that occur.

V. CONCLUSION

Cyber crime is an unlawful act / virtual crime (not real) that utilizes computer media connected to the internet and exploits other computers connected to the internet.

Theory serves as a tool to formulate and understand a problem. In this context, several criminological theories can be used to understand the perpetrators and modes of cyber crime, so that a complete picture of cyber crime and its perpetrators is obtained. There are four theories that can be used to analyze cyber crime, namely anomie, differential association, social control and neutralization.

Because theory is a "tool" then the truth of the contents of a theory can still be debated, denied, contradicted, and perhaps refined based on the results of recent research. So that this study can be an evaluation for legal policy making against cyber crime by paying attention to the applications of criminological theory as an auxiliary science in the development and prevention of crime in the future.

REFERENCES

[1] Santoso , Topo.2020. Criminal Law An Introduction .Depok:Rajawali Perss.
[2] Barda Nawawi Arief, Problems with Law Enforcement and Criminal Law Policy in Combating Crime , Jakarta: Kencana Predana Media Group, 2007
[3] Muladi, Head of Legal Selection for the Criminal Justice System, Publishing Agency, Diponegoro University, Semarang, 2002
[4] T. Subarsyah Sumakara, Law Enforcement (An Approach to Political Law and Criminal Politics), Kencana Utama, Bandung, 2010
[5] Abdul Wahid and Mohammad Labib, Mayantara Crime (Cyber Crime), Jakarta:PT. Refika Aditama, 2005 .
[6] Peter Stephenson, Investigating ComputerRelated Crime: A Hanbook For Corporate Investigators , London New York Washington DC: CRC Press, 2000,
[7] Business fortunacety, Crime , Accessed from http://business.fortunecity.com/buffet/842/art180199_tindakpidana.htm. on May 25, 2017
[8] Djanggih , H. & Qamar, N.(2018). Application of Criminological Theories in Combating Cyber Crime (Cyber Crime). Pandecta Journal. Volumes 13.
[9] Mathilda.F .(2012). CYBER CRIME IN INDONESIA LAW SYSTEM CYBER CRIME IN INDONESIA LAW SYSTEM. Sigma-Mu Vol.4 No.2
[10] Zulhidayat.M .(2016). A CRIMINOLOGICAL REVIEW OF THE “CYBER SEX” PHENOMENON IN THE MAYANTARA WORLD AND ITS LEGAL ASPECTS . (Thesis, University of Muhammadiyah Malang, 2017)