Cyber Crime Prevention Strategy in Indonesia

Yasmirah Mandasari Saragih[1], Andysah Putera Utama Siahaan[2]
[1]*Faculty of Law,* [2]*Faculty of Computer Science*
Universitas Pembangunan Panca Budi
Jl. Jend. Gatot Subroto Km. 4,5 Sei Sikambing, 20122, Medan, Sumatera Utara, Indonesia

Abstract

The development of the Internet and the cyber world did not lead to positive progress. One of the negative things that often happens in the virtual world is cyber crime. The loss of the limits of space and time on the Internet canaffectanything. A cracker can get into a system without an official permit. Some people who infiltrate the system will notify the weaknesses of the system but some of them use the weakness to profit. Several strategies were created to repel the cyber crime. Cybercrime is not only done through the Internet, but this can be done through a network that can transmit signals such as telephone communications. The Indonesian government to apply the law as it applies to online crime. Some of these rules have been applied in the Penal Code, including the Law on Information and Electronic Transactions (UUITE). By implementing this system, the cyber crime cases will be reduced each year.

Keywords— *Cyber Crime, Hacker, Strategy, UUITE, Law*

I. INTRODUCTION

Along with the rapid advancement of information technology, this makes the Internet as a phenomenon in the life of mankind. The Internet, which is defined by the U.S. Supreme Court as: "International Network of Interconnected Computers" has presented the easiness for everyone to either communicate or conduct business transactions anytime and anywhere. There are many ways to interact in cyberspace has been developed [2][3]. An example is the birth of wireless application technology. For example, it allows mobile phones to access the Internet, pay a bank account, book air tickets, etc.

Indonesia conducts technology research in the field of internet quickly. In development, the use of the internet brings many negative sides. It increases the chances for the actions of anti-social and criminal behavior that had been considered unlikely. As a theory says, "Crime is a product of society its self." It means that the community itself that creates crime. The higher the intellectual level of society, the more sophisticated crimes may also occur in the community.

Cybercrime carried out by infiltrating into a computer network system illegally, without permission or the knowledge of the owner of the computer network system is entered [6]. Usually, the perpetrator (Cracker) sabotage or steal the valuable and confidential information. However, some are doing just because he felt challenged to try his skills to penetrate a system that has a high degree of protection. Crime is more prevalent with the development of technology internet/intranet rather than the past.

The Indonesian government will apply the law on cybercrime. A legal entity should work with IT experts to tackle such crimes. To reveal who will be responsible for the crime, an IT expert should be able to perform network forensics to find out the origin and source of the offense. This strategy is expected to reduce or eradicate crimes committed in the world of technology.

II. THEORIES

A. *Cyber Crime*

Currently, the development of technology is increasing rapidly. With the increasing public knowledge about information and communication technology, it brings a lot of positive and negative impacts. In the end, a lot of the man himself who committed abuse in the use of computer technology, which was later increased to a crime in the virtual world, or better known as cyber crime [1]. Cyber crime is a term that refers to criminal activity with a computer or computer network into a tool, target or scene of the crime. Included therein to include an online auction fraud, check forgery, credit card fraud (carding), confidence fraud, identity fraud, child pornography, etc.

In the Internet, security issues are indispensable. For without security, data on existing systems on the Internet can be stolen by irresponsible people. Often an Internet-based network system has flaws or often called a security hole. If the hole is not closed, a thief can enter from the hole. Theft of data and systems from the Internet, including in the case of computer crime. Cybercrime is a crime that is often done on the Internet.

B. *Cyber Crime Types*

Based on the type of activities done, cyber crime can be classified into several types as follows:

1) Unauthorized Access

It is a crime that occurs when someone enters or infiltrate into a computer network system illegally, without permission, or without the knowledge of the owner of the computer network system is entered. Examples of these crimes are Probing and port

2) Illegal Contents

A crime that is done by entering data or information on the Internet about something improper, unethical, and can be regarded as unlawful or disturb the public order, for example, is the spread of pornography or untrue reports.

3) Intentional spread of virus

A spread of the virus is performed by using an email. Often people are exposed to the virus e-mail system is not aware of this. The virus is then transmitted to another place via email.

4) Data Forgery

This type of crime is done with the intention of falsifying data on important documents on the Internet. These documents are usually owned by the institution or institutions with web-based site database.

5) Cyber Espionage, Sabotage, and Extortion

Cyber Espionage is a crime by way of utilizing the Internet to conduct espionage against other parties, by entering into the target computer network system. Sabotage and Extortion is the type of crime committed by creating a disturbance, destruction or the destruction of the data, computer programs or computer network system connected to the Internet.

6) Cyberstalking

This type of crime is done to annoy or harass someone by using a computer, such as using e-mail and be done repeatedly. The crime resembles terror directed against a person by using the internet media. It can happen because of the ease in making an email to a specified address without having to include the identity of the true self.

7) Carding

Carding is a crime that is made to steal credit card numbers belonging to others and used in commercial transactions on the Internet.

8) Hacking and Cracking

The term hacker refers to someone who has a great interest in learning the details of computer systems and how to improve capabilities. Cracking activity on the Internet has a very wide scope, ranging from hijacking an account belonging to someone else, piracy websites, probing, spread the virus, to incapacitate the target.

9) Cybersquatting and typosquatting

Cybersquatting is a crime committed by registering domain names the company of others and then trying to sell it to the company with a more high price. The typosquatting is a crime to make a play domain is a domain that is similar to the domain name of another person.

10) Hijacking

Hijacking is one of the crimes of hijacking other people's work. The most common crime is software piracy.

11) Cyber Terrorism

Measures cybercrime including cyber terrorism if it threatens the government or citizens, including cracking to the government or military.

C. Law on Information and Electronic Transactions (UUITE)

All cyber crime activity requires other activities to launch the intended activity [1][4][5]. Therefore UUITE should be able to cover all of the rules against cybercrime activities. The public should be introduced more and more about the UUITE unambiguous so that people and more about the order regarding this cyber law and help reduce cyber crime activities in Indonesia. The contents of the UUITE threaten the freedom of opinion for a user. An article in UUITE has created to the need for Cyber Law in Indonesia departing from the start number of trade transactions that occur through the virtual world. And in its development, UUITE whose design has been included in the agenda of the House of Representatives since almost ten years ago continues to increase, including protection from hacker attacks, the prohibition of serving content. There are already legal protection in cyberspace.

III. METHODOLOGY

A. UUITE Articles

There are several articles which may have noticed that we look and avoid the snares UUITE. There are about 11 articles that regulate the actions that are prohibited in UUITE, which covers nearly 22 types of conduct prohibited. Of the 11 chapters, there are three suspected articles will jeopardize blogger or Internet surfers unwittingly [1].

Article 27, Paragraph (1) : "Any person intentionally and without the right to distribute and or transmitting and/or make the inaccessibility of Electronic Information and/or Electronic Documents which have a charge of violation of decency."

Article 27, Paragraph (3): "Any person intentionally and without the right to distribute and/or transmitting and/or make the inaccessibility of Electronic Information and/or Electronic Documents which have a charge of insult and/or defamation. "

Article 28, Paragraph (2) : "Any person intentionally and without the right to disseminate information intended to cause hatred or hostility individual and/or a particular group of people based on ethnicity, religion, race and intergroup (SARA)."

For violations of these articles, UUITE sanctions severe enough, as regulated in Article 45 paragraph (1) and (2).

Article 45, Paragraph (1) : "Every person who meets the elements referred to in Article 27 paragraph (1), paragraph (2), paragraph (3), or paragraph (4) shall be punished with imprisonment of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiahs).

Article 45, Paragraph (2) : "Every person who meets the elements referred to in Article 28 paragraph (1) or subsection (2) shall be punished with imprisonment of 6 (six) years and/or a fine of 1,000,000,000.00 (one billion rupiahs). "

B. KUHP Articles

The articles below are intended to protect the cyber law.There are several provisions in force to maintain security in cyberspace.

Article 362 KUHP : Were subjected to carding cases where the offender stole credit card numbers belonging to other people, although not physically because only the card number are using the card generator software on the Internet to conduct transactions in e-commerce. After the transaction and the goods are delivered, then sellers who want to withdraw their money in the bank card was rejected because the owner is not the person making a transaction. Criminal Prison maximum period of 5 years.

Article 406 KUHP : May be imposed in the case of defacement or hacking that make other people's systems, such as a website or program to be not working or can be used as is.

Article 282 and 311 KUHP : May apply to the case of the spread of personal photos or movies on the Internet.

Article 378 KUHP : May be subject to fraud seems to offer and sell a product or goods by advertising in one website so people want to buy and then send the money to the advertiser. But, in fact, the item no. It is known after the money is sent and had commanded the goods did not come so that buyer be deceived.

Article 335 KUHP : Can be subjected to threatening and extortion cases conducted via e-mail sent by the offender to force the victim to do something according to what is desired by the perpetrators and if implemented will bring harmful effects. This is usually done because the perpetrators are usually privy to the victim.

Article 303 KUHP : May be subject to ensnare gambling games are made online on the Internet with the organizers of Indonesia.

C. Legal Basis Handling of Cyber Crime in Indonesia

1) Formal Arrangements Cyber Crime in Indonesia

In addition, to criminalize cyber material, UUITE criminalize cyber-formal, especially in the field of investigation. Article 42 of UUITE provides that the investigation of criminal offenses in UUITE conducted under the provisions of Law No. 8 of 1981 on Criminal Code and the provisions of UUITE [7][8]. That is, the provisions in the Criminal Code investigations remain valid throughout other provisions in UUITE. Specificity UUITE in the investigation include:

- ❖ Investigators who handle cyber criminal act of agency is the National Police or the Ministry of Communication and Information Technology.
- ❖ Investigations carried out with due regard to the protection of privacy, confidentiality, smooth running of public services, data integrity, or the integrity of the data.
- ❖ Atan searches and seizures of Electronic Systems related to an alleged crime should be done by permission of the chairman of the local district court.
- ❖ In conducting the search and/or seizure Electronic Systems, the investigator shall safeguard the interests of maintaining public services.

2) Cyber Crime Setting Petition in Indonesia

Settings cyber criminal offense regulated in Law Number 11 Year 2008 on Information and Electronic Transactions (UUITE). There are several criminal offenses:

- The criminal offenses related to illegal activity, such as:
  - ❖ Distribution or dissemination, transmission, inaccessibility of illegal content, comprising: morality (Article 27 [1] UUITE). Gambling (Article 27 [2] UUITE); insult or libel (Article 27 [3] UUITE); extortion or threatening (Article 27 [4] UUITE). Hoax misleading and harm consumers (Article 28 [1] UUITE); creates a feeling of hatred based on racial intolerance (Article 28 [2] UUITE). Send information containing threats of violence or scare addressed personally (Article 29 UUITE);
    - ❖ In any way to access illegal (Article 30 UUITE).

  - ❖ Illegal interception of the information or electronic documents and Electronic Systems (Article 31 UUITE).

- The criminal offenses relating to interference (interference), such as:
  - ❖ Disruption of the Information or electronic documents (data interference - Article 32 UUITE).
  - ❖ Disruption of the Electronic Systems (system interference - Article 33 UUITE).

- Facilitating criminal acts prohibited (Article 34 UUITE).
- Criminal offense falsification of information or electronic documents (Article 35 UUITE).
- Additional criminal offense (accessoir Article 36 UUITE).
- Weighting against criminal threats (Article 52 UUITE).

IV. EVALUATION

There are several cases happened and its solutions.

A. **Case:** Theft and use of the Internet account belonging to someone else. Account theft is different from physical theft as theft is enough to catch the "user_id" and "password" only. The purpose of the theft is only to steal information only. However, the effect will be felt if the information is used by the parties who are not responsible. It will make all the costs of the use of the account by the thief charged to the actual owner of the account. The case is a lot going on in the Internet Service Provider.

Cause: Forget to logout the account, or easily guessed passwords, such as using the date of birth or relating to the personality or the surrounding environment.

Prevention: Change passwords regularly and use a combination of symbols or letters that are difficult to predict.

B. **Case:** Probing and port scanning. It is the step taken cracker before getting into the targeted server is doing reconnaissance. How that is done is to do a port scanning to see what services are available at the target server. For example, the scanning results may indicate that the target server running Apache web server program, Sendmail mail server, and so on. The analogy of this case with the real world is to look around your house if the door is locked, the key brands are used, where the windows are open, whether the fence is locked (using firewall or not) and so on. Concerned did not perform activities of theft or assault, but the activities are undertaken already suspicious. Whether this can be tolerated or has been within the limits that can not be justified so it can be considered a crime?

Cause: Various programs are used to perform portscanning probing or can be obtained free of charge on the Internet. One of the most popular programs is "nmap" (for systems based on UNIX, Linux) and "Superscan" (for Microsoft Windows-based systems). In addition to identifying the port, nmap also even be able to identify the type of operating system used.

Prevention: Install the firewall and software to detect an intruder.

C. **Case:** Denial of Service (DoS) and Distributed DoS (DDoS) attacks. DoS attack is an attack aimed at paralyzing the target (hangs, crashes) so that he can not provide the service. This attack is not theft, wiretapping, or forgery of data. But with the loss of service target is not able to provide a service so that no financial loss. What is the status of this DoS attack? Imagine if someone can make a bank ATM does not function. Consequently nasabahbank can not perform transactions and bankcan suffer financial losses. DoS attacks can be directed to the server and can also be targeted to the network.

Cause: Tools for doing this widely spread on the Internet. DDoS attack increases this attack to do it from a couple of (tens, hundreds, and even thousands) computers simultaneously. The resulting effect is more powerful than any DoS attack.

Prevention: Install the anti-DoS software.

V. CONCLUSION

Crime in the cyber world that no longer knows no boundaries and raises new issues. The impact has been felt by the community of computer users and networks. Countermeasures meant starting from cyber crime prevention efforts are technological approach with security software, hardware, and then do the socialization efforts of computer and internet in the midst of society, culture approach can also be done by applying ethics. In interacting with other people using the internet, covered by a specific rule called Nettiquette or ethics on the internet. Although there has been no provision is standard on how to interact on the internet ethics, ethics in interacting in the real worldcan be used as a reference In addition to prevention efforts are also made to law enforcement cyber crime. In order to realize the cyber crime law enforcement against crime should be supported by three aspects related to law enforcement, such as legal instruments, law enforcement officers and their application in the field. Aspects instrument is the existence of various laws including UUITE to minimize and can be used as legal protection against prosecution of cybercrime. The presence of UUITE will provide benefits to ensure legal certainty for the people who conduct electronic transactions, fostering economic growth, prevent crime based information technology and protecting public service users by utilizing information technology.

REFERENCES

[1] W. Beneran, "Undang-Undang Cyber Crime," 23 1 2015. [Online]. Available: http://www.totaltren.com/2015/01/undang-undang-tentang-cyber-crime.html. [Accessed 24 12 2016].

[2] Hariyanto and A. P. U. Siahaan, "Intrusion Detection System in Network Forensic Analysis and Investigation," *IOSR Journal of Computer Engineering (IOSR-JCE),* vol. 18, no. 6, pp. 115-121, 2016.

[3] A. Lubis and A. P. U. Siahaan, "Network Forensic Application in General Cases," *IOSR Journal of Computer Engineering (IOSR-JCE),* vol. 18, no. 6, pp. 41-44, 2016.

[4] B. Rahardjo, "Cybercrime," 2012. [Online]. Available: http://keamananinternet.tripod.com/pengertian-definisi-cybercrime.html. [Accessed 24 12 2016].

[5] M. Singh, J. A. Husain and N. K. Vishwas, "A Comprehensive Study of Cyber Law and Cyber Crimes," *International Journal of IT, Engineering and Applied Sciences Research (IJIEASR),* vol. 3, no. 2, pp. 20-24, 2014.

[6] P. D. M. Gercke, Understanding CyberCrime: Phenomena, Challenges and Legal Response, ITU Publication, 2012.

[7] A. Hamzah, Hukum Pidana Yang Berkaitan Dengan Komputer, vol. 35, Jakarta: Sinar Grafika, 1993, pp. 455-462.

[8] Sutarman, Cyber Crime Modus Operasinya dan Penanggulangannya, Yogyakarta: LaksBang Press Indo, 2007.