THE INTERNATIONAL JOURNAL OF HUMANITIES & SOCIAL STUDIES

Violations of Cybercrime and the Strength of Jurisdiction in Indonesia

Masdin Saragih
Lecturer, Faculty of Law, Universitas Simalungun, Simalungun, Indonesia
Henry Aspan
Lecturer, Faculty of Economics and Business, Universitas Pembangunan Panca Budi, Medan, Indonesia
Andysah Putera Utama Siahaan
Lecturer, Faculty of Computer Science, Universitas Pembangunan Panca Budi, Medan, Indonesia
Ph.D. Student, Department of School of Computer and Communication Engineering,
Universiti Malaysia Perlis, Kangar, Malaysia

Abstract:
Cybercrime is a digital crime committed to reaping profits through the Internet as a medium. Any criminal activity that occurs in the digital world or through the internet network is referred to as internet crime. Cybercrime also refers to criminal activity on computers and computer networks. This activity can be done in a certain location or even done between countries. These crimes include credit card forgery, confidence fraud, the dissemination of personal information, pornography, and so on. In ancient times there was no strong law to combat cybercrime. Since there are electronic information laws and transactions, legal jurisdiction of computer crime has been applied. Computer networks are not only installed in one particular local area but can be applied to a worldwide network. It is what makes cybercrime can occur between countries freely. This issue requires universal jurisdiction. A country has the authority to combat crimes that threaten the international community. This jurisdiction is applied without determining where the crime was committed and the citizen who committed the cybercrime. This jurisdiction is created in the absence of an international judicial body specifically to try individual crimes. Cybercrime cannot be totally eradicated. Implementing international jurisdiction at least reduces the number of cybercrimes in the world.

Keywords: *Cybercrime, Jurisdiction, Law*

1. Introduction

Technological advances open up huge crime opportunities. This can be seen from the many cases that come to court about digital crime. The cases handled are about the misuse of technologies such as the internet, hoaxes, fake photos and others. One of the facts that cause cybercrime is the need for computer network technology is increasing. Commercial community activities become important things done by using the computer network. It can be spread all over the country. World activities will last for 24 hours and can be monitored for 24 hours as well. These activities include stock trading, banking, and other financial activities. In cyberspace, any activity can be done. This positively impacts technological advancements and adds convenience for people to exchange information. But this did not escape the negative impact. When pornography rife on the internet, the law can not do much in the past. The development of internet technology triggered the emergence of cybercrime. This action will harm others. Cybercrime activities include credit card theft, hacking multiple sites, intercepting other people's data transmissions, and manipulating data by preparing several programs such as viruses to commit such crimes. Cybercrime has become a threat to international stability, so the government is difficult to compensate crime techniques done with computer technology, especially internet and intranet networks.

Cyberspace is a media without limits because it is connected to a network of computers connected to the world. It does not recognize territorial or state boundaries. This crime will cause its problems, especially in criminal law and jurisdiction. Jurisdiction is the power or competence of state law against people, objects or events. This is the principle of state sovereignty, equality of state and principle of non-interference. Jurisdiction is also a vital and central form of sovereignty that can transform, create or terminate a legal relationship or obligation.

This research tries to explain how the legal system will be applied to cybercrime perpetrators based on certain violations. Each violation has a different legal act. By applying jurisdiction, cybercrime actors will be reduced for the sake of state stability and sovereignty.

2. Theories

2.1. Cybercrime

Cybercrime is an illegal activity conducted in cyberspace with computer intermediaries or other electronic equipment. It includes technologies that support technological means such as mobile phones, smartphones and others that can be done through a global electronic network. Cybercrime attempts to enter a computer network without permission. Cybercrime is considered to conflict or against any applicable law. The difference with a common crime can be seen from the versatile capabilities shown by the development of information and sophisticated communication technology. Figure 1 describes the types of cybercrime.

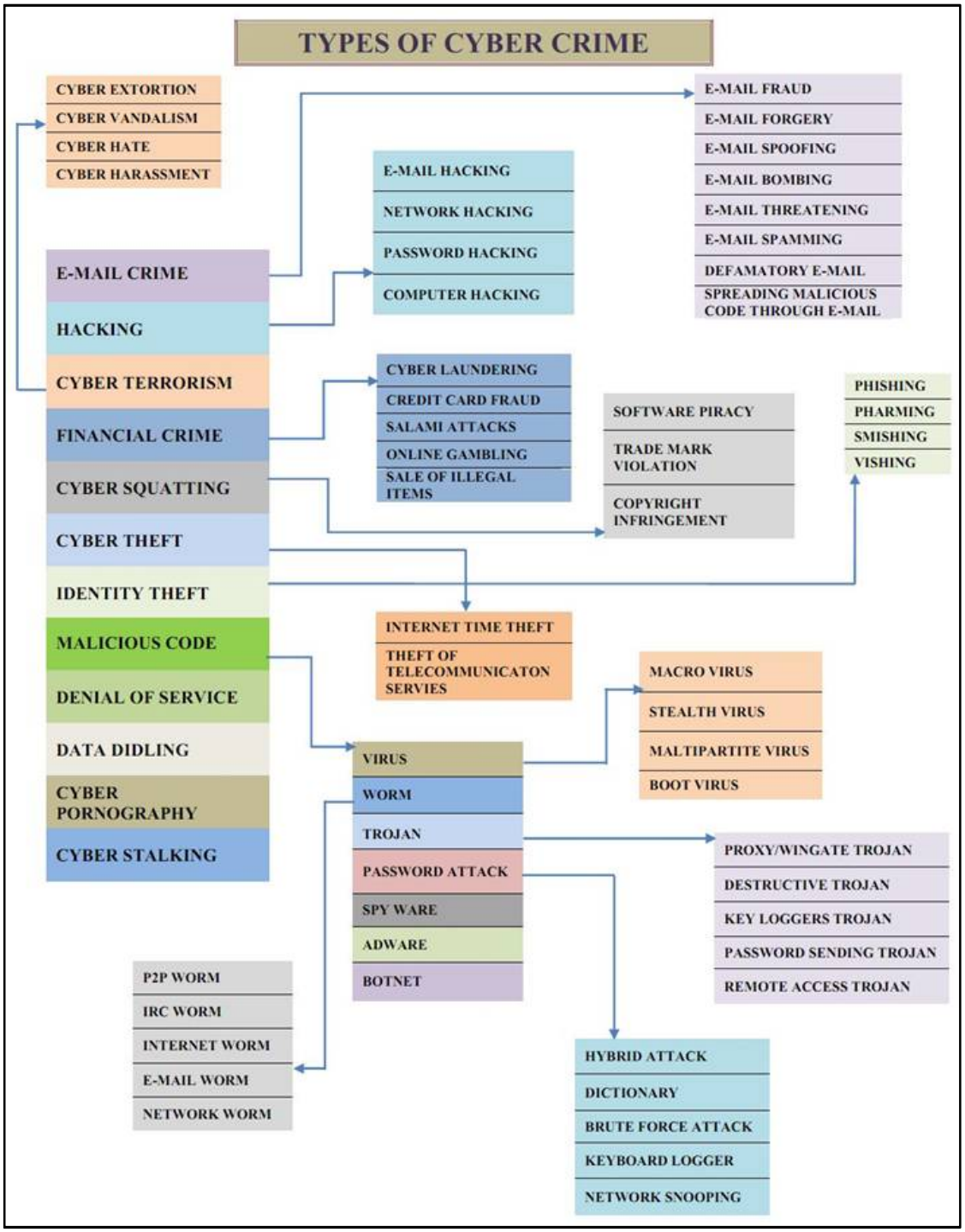

Figure 1: Types of Cybercrime

There are several types of crime on cybercrime that can be classified based on the activities such as:

- Unauthorized Access
  It is a crime that occurs when a person enters or infiltrate into a computer network system unlawfully, without permission, or without the knowledge of the owner of the computer network system it enters. Examples of these crimes are Probing and port.

- Illegal Contents
  It is a crime committed by entering data or information to the internet about a thing that is untrue, unethical, and can be regarded as unlawful or disturbing public order, for example, the spread of pornography or untrue news.

- Virus Spread
  The spread of the virus is generally done by using an email. Often people whose email system is exposed to a virus do not realize this. The virus is then sent to another place via email.

- Cyber Espionage, Sabotage, and Extortion
  Cyber Espionage is a crime by way of exploiting the internet network to conduct spying on other parties, by entering the target computer network system. Sabotage and Extortion is a type of crime committed by making interference, destruction or destruction of a data, computer program or computer network system connected to the internet.

- Carding
  Carding is a crime committed to steal credit card numbers belonging to others and used in trade transactions on the internet.

- Hacking and Cracking
  The term hacker usually refers to someone who has a great interest to learn the computer system in detail and how to improve its capabilities. Cracking activity on the internet has a very wide scope, ranging from hijacking someone else's account, website hijacking, probing, spreading the virus, to the disabling of the target. The latter act is referred to a DoS (Denial Of Service).DoS attack is an attack that aims to paralyze the target (hangs, crashes) so it can not provide services.

- Cybersquatting and Typosquatting
  Cybersquatting is a crime committed by registering the domain name of another company's company and then trying to sell it to the company with a more high price. The typosquatting is a crime by creating a fake domain that is a domain similar to someone else's domain name.

- Cyber Terrorism
  Cybercrime actions include cyber terrorism if it threatens government or citizens, including cracking into government or military sites.

2.2. Constitution of Electronic Information

This law was originally to protect the interests of the state, the public, and the private sector from cybercrime. There are three broad categories that include laws that are about defamation, blasphemy, and online threats.The law ensnares not only the author but also those who distribute, transmit, or otherwise make the content accessible electronically. The mistake is to distribute is to send and disseminate information and electronic documents to many people or various parties through the internet network. Transmitting is sending information directed to one party through the virtual world. Making publicly accessible content is all other cybercrime deeds. Those who share information or content that violates the law may be charged and penalized. Social media users should be more careful and do not share things publicly without good and correct verification. The information should be reexamined before it is fully shared publicly. Sharing, distributing and harming others is a criminal act that can be criminalized. The following are some restrictions that must be considered in using information in the scope of cyberspace.

- Create and grant access to ethically charged content
  Any person who knowingly distributes, transmits, and or creates content that has an electronic infringement charge that is accessible electronically can be charged under this Act.

- Threaten, blackmail and defame a person's name
  Any person who distributes, transmits and makes accessible electronic information possessing defamation or defamation contents outlined in the Criminal Code may be charged under this article.

- Tapping
  Tapping can only be done for the purpose of investigating law enforcement officers. The intercepts referred to are those for

listening, recording, deflecting, altering, inhibiting, and recording non-public information, using either a wired communications network or a wireless network, such as electromagnetic or radio frequency.

- Defamation
  Any person intentionally and without the right to distribute, transmit and make such information publicly accessible shall be subject to criminal penalties.

- Hoax
  This type of prohibition to provide false news that is provocative and misleading which resulted in the loss of consumers can be punished with imprisonment.

- Hate Speech
  Threats of disseminating information aimed at generating a sense of hatred or hostility towards specific individuals or groups of people based on ethnicity, religion, race, and intergroup including things that can be criminalized.

3. Result and Discussion

3.1. Crime Jurisdiction in Cybercrime Transaction

Cybercrime is an illegal activity conducted in cyberspace with comp

Jurisdiction is a state's authority to exercise its national law against persons, objects, or legal events. State jurisdiction in international law means the right of a State to regulate and influence by legislative, executive, and judicial measures and actions on the rights of individuals, property or property, behaviors or events which are problems within a country and abroad.

Jurisdiction relates to legal matters, the powers or authorities of a judiciary or other legal entity which is based on applicable law. There are limits to the scope of that ability to create, implement and apply the law to those who disobey it. Although jurisdiction is closely related to territory, this linkage is not absolute. Other states may also have authority to try an act done abroad.

The jurisdiction of the law has always been a serious problem faced by law enforcers especially if the offender is a foreign citizen. Cybercrime and jurisdiction make it clear that to address cybercrime problems within this legal jurisdiction involving inter-state. Several components can be used by states to claim legal jurisdiction over cybercrime cases:

- Place of crime conducted
  This is usually done by applying the principle of territoriality by factors such as:
  - The locations where crime is committed
  - The location where the evidence is located
  - The locations where the offender is located
  - The location where the result is located
  - The locations where the matters related to the crime is located

- The Place where the perpetrator was arrested
  This component is used by applying the principle of universality in which each State has the right to try any person who commits an international crime.

- Citizenship
  This component is divided into two, citizenship of victims and perpetrators. The victim's citizenship may be used to claim the jurisdiction of a case and the perpetrator's citizenship may also be used but the offending State must guarantee to prosecute justly the offender for feeling responsible for the acts perpetrated by the offender.

- The strength of the case
  This component should be submitted by the public prosecutor in a document stating that they have a strong case to prosecute the perpetrator in his country.

- Criminalization
  The duration of the crime can be used as a component to determine jurisdiction in the case of cybercrime.

- Justice and Comfort
  Justice aims to state the right to claim jurisdiction over cybercrime cases. The country has a fair, impartial and comfortable judicial system for witnesses to attend the hearing.

3.2. Law Enforcement

Law enforcement on cybercrime especially in Indonesia is strongly influenced by five factors such as law, mentality, social behavior, means, and culture. The law cannot be upright by itself always involves humans in it and also involves human behavior in it. The law also can not erect by itself without any law enforcers. Law enforcers are not only prosecuted for professionalism and smart in applying legal norms but also dealing with someone even a group of people suspected of committing a crime.

Law enforcers are required to work hard because law enforcement is the main subject of war against cyber crime. For example, UN Resolution No. 5 of 1963 on efforts to combat crimes of misuse of Information Technology on December 4, 2001, indicates that there are a severe, grave and immediate international problem. The Criminal Code is still used as the legal basis to encompass cybercrime, especially the cybercrime which fulfills the elements in the articles of the Criminal Code. Some of the constitutional grounds in the Criminal Code used by law enforcement agencies include:

- Article 167 of the Criminal Code
- Article 406 paragraph1 of the Criminal Code
- Article 282 of the Criminal Code
- Article 378 of the Criminal Code
- Article 112 of the Criminal Code
- Article 362 of the Criminal Code
- Article 372 of the Criminal Code

There is another law related to this matter. It is Law No. 11 of 2008 on Information and Electronic Transactions (IET). The rules of criminal acts committed therein are proven 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 the alliance do at least there have four people who called the police and became a suspect for allegedly committed a crime stipulated in the Law on ITE. The suspects or victims of the ITE Act are active internet users who are accused of insulting or related to the contempt content on the internet.Those accused under the IET Law are likely to be subject to Article 27 paragraph 3 in conjunction with Article 45 paragraph 1 of the IET Law which is six years in jail and 1 billion rupiahs fine. IET law can be used to beat all cybercrime activities on the internet without exception.

3.3. Legal Sanctions

Several laws govern the penalties for cybercrime perpetrators. Here are some of the laws that serve as the reference of the state of Indonesia in regulating the punishment of cybercrime perpetrators:

1. Law No. 19 of 2002 on Copyright. According to Article 1 of Law No. 19 of 2002 on Copyrights stated that a computer program is a set of instructions embodied in the form of a language, code, scheme or another form. When combined with a computer software, it is capable of making the computer work to perform functions, special functions or to achieve specific results, including preparation for designing such instructions. The copyright for the computer program is valid for 50 years, as contained in Article 30. The price of a costly computer or software program for Indonesian citizens is a promising opportunity for businesses to double and sell pirated software at very low prices.
2. Law No. 36 of 1999 on Telecommunications. According to Article 1 of Law No. 36 of 1999, Telecommunications is any transmission, transmission, and acceptance and any information in the form of signs, signals, writings, drawings, sounds and sounds through a wire, optical, radio, or other electromagnetic systems. From the definition, the Internet and all its facilities is one form of communication tool because it can send and receive any information in the form of images, sounds, and films with electromagnetic systems. Misuse of the Internet disturbing public or private order may be penalized by using this Act:
   - Illegal access, acts of unauthorized access to this computer system has not been regulated in the legislative system in Indonesia. Article 22 number 36 year 1999 concerning Telecommunication may be applied. Article 22 of the Telecommunications Law states that everyone is prohibited from doing unlawful, unlawful, or manipulating acts:
     a. Access to telecommunication networks
     b. Access to telecommunication services
     c. Access to dedicated telecommunication networks.

     Article 50 of the Telecommunications Law provides a criminal penalty against anyone who violates the provisions of Article 22 of the Telecommunications Law with a maximum imprisonment of six years or a maximum fine of Rp. 600,000,000.00.
   - Illegal interception of computer operations, systems, and computer networks. Article 40 of the Telecommunications Law may apply to this type of interception. Article 56 of the Telecommunications Law provides a criminal penalty against anyone who violates the provisions of Article 40 with a maximum imprisonment of 15 (fifteen) years.
3. Law No. 8 of 1997 concerning Company Documents. By the issuance of Law no. 8 of 1997 dated March 24, 1997, concerning Company Documents in the provisions of one of its articles regulates the possibility of storing corporate documents in the form of electronic (paperless) acknowledging that company documents stored in electronic media can be

used as valid evidence. For example, Compact Disk Read Only Memory (CD ROM), and Write Once Read Many (WORM), outlined in Article 12 of the Act as valid evidence.

4. Law No. 25 of 2003 on Amendment to Law no. 15 year 2002 on the Crime of Money Laundering. This law is the most powerful law for an investigator to obtain information about a suspect who commits fraud over the Internet since it does not require long and time-consuming bureaucratic procedures since fraud is one of the types of crimes included in the washing money as contained in article 2, paragraph 1. The Investigator may request to the bank receiving the transfer to provide the identity and banking data owned by the suspect without having to follow the rules as stipulated in the Banking Act. In the Banking Act the identity and banking data is part of bank secrecy so that if the investigator needs the information and data, the procedure to be done is to send a letter from the Chief of Police to the Governor of Bank Indonesia.

4. Conclusion

Cybercrime is a crime arising from the negative impact of technological development. Means used in the form of computers, smartphones, and devices connected to the Internet. It also occurs because of the inability of the law including the apparatus in reaching it. This crime is virtual because the offender does not appear physically.Cybercrime law enforcement is an activity that harmonizes the values that are outlined in the law against cybercrime. Cybercrime is an unlawful activity conducted using the internet based on the sophistication of computer technology and telecommunications.Jurisdiction in cyberspace requires clear principles rooted in international law. Each country may develop regulations to adopt the same solution to statements concerning internet jurisdiction. The principles of jurisdiction will make it easier for states to enter into cooperation to harmonize criminal provisions to cope with cybercrime.Indonesia has implemented a strong jurisdiction system in tackling cybercrime. These provisions have been regulated in the Criminal Code as appropriate. Under applicable law, cybercriminals will be prosecuted by the provisions.

5. References

i. Brown, C. S. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology, 9*(1), 55-119.

ii. Hait, A. A. (2014). Jurisdiction in Cybercrimes: A Comparative Study. *Journal of Law, Policy and Globalization, 22*, 75-84.

iii. Hariyanto, & Siahaan, A. P. (2016). Intrusion Detection System in Network Forensic Analysis and Investigation. *IOSR Journal of Computer Engineering, 18*(6), 115-121.

iv. Manurung, D. (2013, 11 27). *Cyber Crime: Hukum dan Sanksi*. (Blogspot) Retrieved 12 10, 2017, from http://desrianimanroe.blogspot.co.id/2013/11/hukum-dan-sanksi.html

v. Muslimah, S., & Hidayati, N. (2017, 9 29). *7 Hal di UU ITE yang Wajib Kamu Tahu Agar Tak Bernasib Seperti Jonru*. (Kumparan) Retrieved 12 20, 2017, from https://kumparan.com/@kumparannews/7-hal-di-uu-ite-yang-wajib-kamu-tahu-agar-tak-bernasib-seperti-jonru

vi. Ramadhani, S., Saragih, Y. M., Rahim, R., & Siahaan, A. P. (2017). Post-Genesis Digital Forensics Investigation. *International Journal of Scientific Research in Science and Technology, 3*(6), 164-166.

vii. Rusmiatiningsih. (2013, 10 19). *Yuridiksi Hukum Pidana dalam Transaksi Cybercrime*. (Blogspot) Retrieved 12 20, 2017, from http://rusmiatiningsih.blogspot.co.id/2013/10/yuridiksi-hukum-pidana-dalam-transaksi.html

viii. Saragih, Y. M., & Siahaan, A. P. (2016). Cyber Crime Prevention Strategy in Indonesia. *International Journal of Humanities and Social Science, 3*(6), 22-26.

ix. Sudyana, D. (2015, 10 1). *Pengenalan Cyber Crime*. Retrieved 12 20, 2017, from http://blog.didiksudyana.com/2015/10/pengenalan-cyber-crime.html

x. Tasril, V., Ginting, M. B., Mardiana, & Siahaan, A. P. (2017). Threats of Computer System and its Prevention. *International Journal of Scientific Research in Science and Technology, 3*(6), 448-451.

xi. Triwahyuni, Y. (2015, 12 5). *Pengertian, Jenis-jenis, dan Contoh Kasus Cyber Crime*. (Wordpress) Retrieved 12 20, 2017, from https://yuliatwn.wordpress.com/2015/12/05/pengertian-jenis-jenis-dan-contoh-kasus-cyber-crime/