Implementation of Organized Cyber Crime Countermeasures Against National Investment

Dwi Putri Melati[1*]   Nikmah Rosidah[2]   Heni Siswanto[2]

1.Students of the Doctoral Study Program in Law, University of Lampung. Lecturer of the Faculty of Law, Universitas Sang Bumi Ruwai Jurai, Bandar Lampung, Indonesia

2. Lecturer of Faculty of Law, Universitas Lampung, Bandar Lampung, Indonesia

Abstract

Internet abuse is also evidenced by the frequent discovery of crimes through the internet network. Internet abuse is also evidenced by the frequent discovery of crimes through the internet network. The implementation of online transactions there are also those who use social media, but many parties who abuse social media transactions as well as fraud crimes. Misuse of crimes against matters related to data and systems on computers should get special attention because it is related to confidentiality. The implementation of organized cyber crime countermeasures against national investments can be in the form of improvement of legal tools, education and training of traditional human resources, researchers' abilities, evidence tools and inadequate computer tools. To overcome the obstacles identified in cybercrime investigations, legal instruments, researcher training, appropriate facilities can be built, enhance an international investigation and participation effort, and make efforts to get out of cybercrime. The legal system in Indonesia does not separately manage computer crime through the internet world. Obstacles found in cybercrime investigations include related to legal issues.

Keywords: Implementation, Cyber Crime, Countermeasures.

DOI: 10.7176/JLPG/115-06

Publication date: November 30th 2021

1. Introduction

In the era of the development of the electronic age emerged a new era, namely the era of information technology. The era of information technology is demonstrated by the shift of traditional industries to economic industries using the digitization of information. This information technology era is often referred to as the digital revolution through technological shifts and shifts in communication tools. The Internet is the technology of information and communication that is most commonly encountered in a human activity. The Internet becomes a pimadona for surfing in cyberspace without any restrictions then the network is very accessible.

Globalization encourages the birth of information technology development, this phenomenon is very fast happening throughout Indonesia and parts of the world both developed countries to developing countries. Thus making information technology as an effort to advance nations and countries into one way to get world information quickly and accurately, the era of globalization like today humans around the world can exploit internet technology. Through the internet network a variety of information and various types of intermezo, communicating online with people far from our location. This era of globalization in addition to information technology is used to advance the nation there are also bad influences in human life. At this time humans get many benefits and benefits with the development of the era of information globalization, we get in accessing information through information technology.

Everyone is easy to master technology, the real negative impact occurs with various forms of cyber crime, it becomes a result and target on the globalization of information with various technological products such as the very well known mobile phones or what we often know with mobile phones, making it very easy for humans to access information that can also facilitate cyber crime. But the development of the internet is widely abused by irresponsible individuals who can lead to the loss of a country's identity. At this time, with internet access that is very easy to access anytime, anyone and anywhere, minors can access the internet through their mobile phones and then see the sites spread on social media that tell the problems of adulthood. Thus causing unexpected consequences such as the imitation of negative things that he has seen, which causes negative impacts for the nation's successors. Internet abuse is also proven by frequently found crimes through the internet network. Like online buying and selling transactions that are often misused by individuals to commit crimes. One of the crimes is fraud. Fraud not only occurs on the internet but also occurs other telecommunication networks, namely through mobile phones, the perpetrators do everything they can to carry out their crimes, looking for victims' data up to the problems that are being faced by victims. **So the author created a scientific work with the title "IMPLEMENTATION OF ORGANIZED CYBER CRIME COUNTERMEASURES AGAINST NATIONAL INVESTMENT".**

2.   Results And Discussion

Cybercrime is a type of crime activity in online media or cyberspace by using the main means of sophistication of computer technology by using internet tools and networks as its medium. Cybercrime is a crime that has a cross-border nature, meaning this crime can occur anywhere and occurs in various countries and can occur at any time. Cybercrime also has two meanings. In a broad sense, cyber crime is all illegal acts committed over computer networks and the internet to profit by harming others. In a narrow sense, cybercrime is all unauthorized activity or illegal action to attack or damage a computer's security system and also data processed using a computer system.[1] In the opinion of experts, the notion of cybercrime, as follows:

1.   Parker argues that cybercrime is an act or event related to computer technology.
2.   Wahid and Labib explained that cybercrime is all types of use of computer networks for criminal purposes and misuse of the ease of digital technology.
3.   Widodo argued that cybercrime is activities that use computer networks in committing crimes, bias also makes computers a target for crime.
4.   The Organization of European Community Development (OECD) explains that cybercrime is all illegal access to data transmission. That is, all unauthorized activities in a computer system including a crime.

Cybercrime is also commonly done in various ways and various purposes. Cyber crime is widely done by people who understand and master / experts in the field of information technology. Therefore, there are forms and characteristics of cybercrime:[2]

Forms of Cybercrime

Some of the differences in forms of cybercrime related to the use of information technology by using computer facilities and online media. Including:

1.   Accessing to systems and services that aim for sabotage or data theft, and can also be falsification of important and confidential information.
2.   Illegal Content, such as hoaxes, slander, pornography.
3.   Illegal access by opening or forcing entry to someone else's account without permission
4.   Sabotage and Extortion

Characteristics of Cybercrime

The characteristics of cybercrime concern several things including:[3]

a.   Scope on crime
b.   Crime is nonviolent (without violence) so there is no visible chaos.
c.   The perpetrators of this crime are universal.
d.   This mode of crime is included in the *modus operandi*.
e.   The type of loss is material or non-material.

As the phenomenon that has occurred in Indonesia is used as the headquarters of the perpetrators to carry out their crimes, it is proven that the Metro Jaya Police has arrested 85 Chinese Foreign Nationals who formed an online fraud syndicate that uses mobile phones as a tool to commit fraud against Foreign Nationals from China both abroad and inside Indonesia.

The revelation of this online media fraud case began because of information from the police of the People's Republic of China (PRC) who reported about fraud that had been committed in Indonesia. Metro Jaya Police has conducted simultaneous raid operations in several regions including Jakarta, Tanggerang to Malang. From the operation, the police have arrested as many as 91 suspected perpetrators of fraud through online media (cybercrime). 85 of them were Chinese foreigners and 6 Indonesian citizens, as of Monday afternoon, November 25, 2019.[4]

One of the points of the raid was in the city of Malang, as many as 8 houses are raided related to international cyber crime cases. The house is spread in several residential areas of dieng, puncak dieng, ijen nirwana and a house at the top of yamin tidar malang city. All houses in the elite area are contracted by a syndicate of online media-based fraudsters.

Kombes Pol Frans Barung said that its members were assisted by the police *satreskrim* malang and 15 chinese state police who took part in the process of searches of evidence. The evidence included 32 mobile phones, 10 iPads, two CCTV footage, six passports, an internet modem, and two laptops. This evidence is obtained from several different locations. [5]

[1] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)* (Jakarta: PT. Refika Aditama, 2005). hal.. 40
[2] Muhammad Prima Ersya, 'Permasalahan Hukum Dalam Menanggulangi Cyber Crime Di Indonesia', *Journal of Moral and Civic Education*, 1.1 (2018), 50–62 p 53-54 <https://doi.org/10.24036/8851412020171112>.
[3] DEWI MUSTARI, 'Cyber Crime: Penggunaan Skimmer Terhadap Pembobolan Atm', *Faktor Exacta*, 8.3 (2015), 261–65 p 262 <https://journal.lppmunindra.ac.id/index.php/Faktor_Exacta/article/view/326>.
[4] TOTOK WIJAYANTO, 'Penipu Warga Negara China - Kompas.Id', *Kompas*, 2019 <https://www.kompas.id/label/penipu-warga-negara-china> [accessed 1 October 2021].
[5] Darmadi Sasongko, '8 Rumah Di Malang Digerebek Terkait Kejahatan Cyber Crime Internasional | Merdeka.Com', *Merdeka.Com*, 2019 <https://www.merdeka.com/peristiwa/8-rumah-di-malang-digerebek-terkait-kejahatan-cyber-crime-internasional.html> [accessed 1 October

While the 6 Indonesians who were caught have been used as witnesses, according to the confessions of 6 Indonesian citizens only helped the perpetrators (Chinese nationals) during their stay in Indonesia. These six Indonesian citizens help the perpetrators to walk around, travel, help prepare meals to clean the house rented by Chinese nationals. In addition, these perpetrators come to Indonesia only using tourist visas, they will return to their country for 3 months to renew or extend the visa. From the results of the examination, these perpetrators claimed to be members of the police and prosecutors to help the victims in solving tax problems, as well as bankers who offered investments. This syndicate commits fraud through the Indonesian state telephone connection, they often contact their victims who are abroad and then they offer the services of perpetrators who claim to be able to take care of all victims' problems such as tax payments. Victims who feel interested will then send money in accordance with the consent of the perpetrators. The perpetrators claimed they already knew first who the victims were in trouble, as great as the perpetrators were to know the database of anyone who was troubled to be able to reap profits worth Rp. 36 Billion from victims who were in China. Currently, an investigation is still being conducted on the case and it is not yet clear about the laws and regulations governing the case. From the discussion above, the process of eradicating cyber crime cases related to legal policy is to form criminal law legislation that is part of criminal policy by trying to protect the public so that criminal law policy includes efforts to achieve community welfare. The basis of criminal law policy is the Criminal Code and the Law.

Cyber crime is stipulated in Article 378 of the Criminal Code, reads:
"Whoever with the intention to benefit himself or others by going against the law, by using false names or false dignity, by deception or by a series of lies moves others to hand something to him, or to give up debts or eliminate receivables, is threatened with fraud with a maximum imprisonment of 4 years.".

While in article 28 paragraph (1) of the ITE Law reads:
"Everyone intentionally without the right to spread false and misleading news resulting in consumer losses in Electronic Transactions".

Based on the legal policy in the form of criminal code and other laws, it is considered necessary for law enforcement or authorities to combat cyber crime. Law enforcement is something that can affirm legal systems in order to run smoothly in order to build universality. The existence of law enforcement in one country, the legal system in the country can run properly.

In this case, the law enforcement in question is the State Police of the Republic of Indonesia, in cyber countermeasures we can see the role of the Republic State Police responsible for law enforcement of cyber crime crimes, As article 13 in Law No. 2 of 2002 concerning the Police of the Republic of Indonesia among others: "Maintaining the security and order of the community, upholding the law, providing protection, protection, and service to the community".[1]

Organized crime based on cyber crime is an unusual form of crime, even the crime can not only harm society alone, but can cause harm, even the peak can destroy a country. Where this crime can break into the resilience and defense of a country or can leak documents that are state secrets, for it is considered necessary special efforts in eradicating it, the Police in this case is one of the state institutions that have the authority in dealing with organized crime based on cyber crime, it has become an obligation to strengthen the efforts of the Police in combating cyber crime-based organized crime, One of them by giving the breadth of space for the police through a special form of regulation. Then it can be spelled out more deeply the stages of police performance in terms of eradication with certain regulatory derivatives, in this case can be clarified.

That legislation is needed that specifically regulates cybercrime and then forms a derivative of the law that can describe the efforts of the police in combating such crimes. So that with the Law that regulates specifically the act of Cyber Crime, the State Police of the Republic of Indonesia can achieve and realize its main task of Protecting and Protecting the community.

Legal policies are used as an alternative to solving social problems. The management of social problems is carried out by law enforcement which is a reference for crimes committed by national and international communities. As one of the references to the problem, legal policy also has limitations in tackling crime because it is very broad and complex.

The renewal of criminal law (penal reform) according to Barda Nawawi Arief, is as follows: [2]

1. Policy approach:
   a. Part of social policy;
   b. Part of the criminal policy;
   c. As part of law enforcement policy;
2. Viewed from the point of view of value approach

2021].

[1] Pasal 13, 'Undang-Undang Republik Indonesia Nomor 2 Tahun 2002 " Tentang Kepolisian Republik Indonesia" Lembaran Negara RI,' 2002.

[2] barda nawawi arief, *Bunga Rampai Kebijakan Hukum Pidana* (jakarta: Kencana prenada media grup, 2008).p 29

In essence, the renewal of criminal law is an effort to review and reassess reorient and reevaluate, sociopolitical, sociofilosophys and sociocultural values that underlie criminal policy and provide content to the normative and substantive content of the criminal law that is aspired to.

According to Roeslan Saleh, he stated several related matters still needed criminal and criminal law, as follows: [1]

   a. The need for criminal law lies in the consideration between the value of that outcome and the value of the boundaries of individual freedom.

   b. The need for improvement or treatment of the condemned, then there is a reaction to violations of these norms..

   c. Criminal or criminal law influence is not solely aimed at the criminal, but also to influence people who are not evil, namely citizens who obey the norms of society..

Therefore the use of criminal law on crime prevention is still needed at this time, because criminal law has a repressive side and also a preventive side. It means that people who obey the law and do not participate in doing or will think twice if they want to commit a crime. Sajipto Rahardjo explained that law enforcement is a stage in realizing the wishes or minds of lawmakers formulated in the rules of law. In general, enforcement is an action / effort in the use of legal devices to implement / impose legal sanctions to ensure the implementation of the provisions set by. [2]

Furthermore, Soerjono Soekanto explained that law enforcement lies in activities that spread the relationship of values that are spelled out to good rules for reassuring and prospering human life.

Meanwhile, the success produced by law enforcement there are several factors in it, namely:[3]

  a) Rules of the Law

  b) Law enforcement.

  c) The community acts as a supporter in enforcing the law.

  d) The Existence of Supporting Facilities and Facilities to Enforce the Law

  e) Cultural Factors, consisting of Copyright, Works, and Karsa that exist in life

These factors are interrelated and are the essence and benchmark of the effectiveness of law enforcement. In a developing country, the function of law is not only as a tool of social control solely but as a guideline for society in building renewal in social life and so on. As should law enforcement be applied. Law enforcement is a symbol that strengthens the rule of law system that includes good values. Law enforcement is an attempt to make the ideas and concepts of law that people expect to become a reality. Law enforcement is a process that involves many things.[4]

3. Conclusion

Victims assume or stigmatize that the perpetrators of cybercrime are criminals. Cybercrime models vary and develop following technological developments, but if observed it will be seen if this activity has the same nature as conventional crime. But the main difference is that cybercrime uses computers in its implementation. Crimes related to the confidentiality, integrity and existence of data as well as computer systems get special attention, because these crimes have a different character from conventional crimes. The legal system in Indonesia has not specifically regulated computer crimes through internet media. Some existing regulations inside and outside the Criminal Code can be applied to certain temporary violations, but there are also violations that cannot be expected under current law. Obstacles to efforts to investigate cybercrime include problems with legal organs, investigators' capabilities, evidence tools and inadequate computer facilities. To overcome the obstacles identified in cybercrime investigations, efforts can be made, among others, to improve legal instruments, train researchers, build appropriate facilities, enhance international research and cooperation efforts and prevent cybercrime.

Reference

Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)* (Jakarta: PT. Refika Aditama, 2005)

Arief, Muladi dan Barda Nawawi, *Teori-Teori Dan Kebijakan Pidana* (bandung: alumni, 2010)

barda nawawi arief, *Bunga Rampai Kebijakan Hukum Pidana* (jakarta: Kencana prenada media grup, 2008)

Dellyana, Shant, *Konsep Penegakan Hukum* (yogyakarta: liberty, 1988)

Ersya, Muhammad Prima, 'Permasalahan Hukum Dalam Menanggulangi Cyber Crime Di Indonesia', *Journal of Moral and Civic Education*, 1.1 (2018), 50–62 <https://doi.org/10.24036/8851412020171112>

Mustari, Dewi, 'Cyber Crime: Penggunaan Skimmer Terhadap Pembobolan Atm', *Faktor Exacta*, 8.3 (2015), 261–65 <https://journal.lppmunindra.ac.id/index.php/Faktor_Exacta/article/view/326>

---

[1] Muladi dan Barda Nawawi Arief, *Teori-Teori Dan Kebijakan Pidana* (bandung: alumni, 2010). p 153

[2] Satjipto Rahrjo, *Masalah Penegakan Hukum* (sinar baru, 1983). p 24

[3] Soerjono Soetanto, *Faktor – Faktor Yang Mempengaruhi Penegakan Hukum* (Jakarta: raja grafindo persada, 1983). p 5

[4] Shant Dellyana, *Konsep Penegakan Hukum* (yogyakarta: liberty, 1988). p 37

Rahrjo, Satjipto, *Masalah Penegakan Hukum* (sinar baru, 1983)

Soetanto, Soerjono, *Faktor – Faktor Yang Mempengaruhi Penegakan Hukum* (Jakarta: raja grafindo persada, 1983)

Perundangan- undangan

Pasal 13, 'Undang-Undang Republik Indonesia Nomor 2 Tahun 2002 " Tentang Kepolisian Republik Indonesia" Lembaran Negara RI,' 2002

Internet

Sasongko, Darmadi, '8 Rumah Di Malang Digerebek Terkait Kejahatan Cyber Crime Internasional | Merdeka.Com', *Merdeka.Com*, 2019 <https://www.merdeka.com/peristiwa/8-rumah-di-malang-digerebek-terkait-kejahatan-cyber-crime-internasional.html> [accessed 1 October 2021]

Wijayanto, Totok, 'Penipu Warga Negara China - Kompas.Id', *Kompas*, 2019 <https://www.kompas.id/label/penipu-warga-negara-china> [accessed 1 October 2021]