ISSN: 2963-931X
**International Conference Restructuring and Transforming Law 2022**
Volume 1 Issue 1,
(icrtlaw@ums.ac.id)

# Cybercrime": The Phenomenon of Crime through the Internet in Indonesia

Yoga Pratama[1], Krisna Indra Sakti[2], Firmawan Setyadi[3], Nur Ahmad Azi Ibrahim[4], Ali Mukti Nur Hidayat[5]
[1] Muhammadiyah University of Surakarta (C100190359)
[1] Muhammadiyah University of Surakarta (C100190383)
[1] Muhammadiyah University of Surakarta (C100192243)
[1] Muhammadiyah University of Surakarta (C100192351)
[1] Muhammadiyah University of Surakarta (C100192036)

**ABSTRACT**

Technology has long been thought to have two faces: good and bad. Everyone understands the importance of technological progress. However, few people are aware of the negative consequences of technology. The discussion of this article on cybercrime shows how crime has become more sophisticated as a consequence of technical instruments. Cybercrimes, which are simply defined as illegal acts committed through the use of computers or the Internet, have created new dilemmas for politicians and law enforcement officers. Carding has become a serious problem in Indonesia and must be addressed immediately. Hacking and vandalism are two more types of cyber crimes that often occur in Indonesia. Despite the fact that the estimated number of Internet users in Indonesia (4, 38 million people) less than 5% of the entire population, cybercrime should be taken seriously by everyone. Cybercrime has grown to incomprehensible proportions, posing a hazard to public safety in the flow of communications and information.

**Keywords**: "cybercrime", virtual reality, infinite world

## INTRODUCTION

**lowest social. This is known as white collar crime. Jo Ann L. MillerThe Internet: The Technology That Created a "Cyber" World**

People's ideas about life have shifted as a result of the introduction of modern communication technologies such as the internet. Economic operations, business, social engagement, and politics all require a paradigm shift in human communication. People used to be controlled by face-to-face physical acts. Humans are bound by several factors. The Internet removes the boundaries of human location, distance, and time. According to Kenichi Ohmae, this is an infinite universe (Mahayana, 1999: 97).

The Internet is a network of millions of interconnected computers. Anyone with an internet connection can communicate with anyone on earth just by using a keyboard and mouse in front of them. Every information need can be met easily. Many people use it because of the convenience it provides. When compared to radio and television, internet penetration among the general public is among the fastest. Internet gained 50 million users in less than five years, while radio took 38 years and television took 13 years (Temporal & Lee, 2002: 7). An estimated 220 million people currently use the internet.

By leveraging the internet, users can go on adventures, travel, and explore the entire virtual world, the realm of computer-mediated communication. Virtual reality available; cannot be captured or held with one hand, but socially constructed by those involved in communication and information technology. Cyberspace is a strange and fake (hyperreal) domain. According to Piliang, engineering covers the (actual) world with authentic signs in such a way that the boundary between sign and reality, between model and reality, is destroyed (2001).

People can get everything they need online, including entertainment, benefits, and convenience, without ever leaving their homes. You can get free information from local and worldwide media at no charge. You can listen to music without buying a cassette. Various types of books are made accessible to lecturers without forcing them to leave the classroom. This is the "technology hangover zone" proposed by Philips and Naisbitt (2001).

The virtual life provided by cyberspace has given birth to various new recreational activities, such as teleshopping, teleconference, virtual galleries, virtual museums, and e-commerce, but has also given birth to deviance, such as online crime or cybercrime.

**"Cybercrime": A Form of Crime in Cyberspace**

Cybercrime Cybercrime is also referred to as a computer crime in certain publications. The US Department of Justice defines computer crime as "...any criminal act involving knowledge of computer technology for its commission, investigation, or prosecution." It is defined as "any illegal, unethical or inappropriate activity related to the automated processing and/or transmission of data" by the Organization for the Development of the European Community. "In general, cybercrime can be characterized as the unlawful use of a computer," explains Hamzah (1989).

According to Wisnubroto (1999), computer crime is defined as a crime committed by using a computer as a means/tool or as an object, for profit or not, to the detriment of third parties, depending on several elements listed above. In short, computer crime is defined as any illegal activity carried out using modern computer technology. Furthermore, since the crime occurred in cyberspace via the internet, the term "cybercrime" was born.

Most people who are familiar with communication technology (telecommunication) have heard the term "cybercrime". Cybercrime, often known as cybercrime, is a well-documented phenomenon. It's magical, but it's also not. Many cybercrime incidents occur regularly, especially in countries where there is no legal clarity in the field of modern communication technology (convergence).

Communication technology that has the potential to drastically affect human communication behavior has an "evil side" in addition to providing benefits such as increasing the ease of communication. One of the drawbacks of technology is that it makes it easier for “criminals” to commit crimes. Due to modern technology, cyber fraudsters can prey on their victims. Despite their desire not to be labeled as criminals, their actions put them in the same category.

According to Rahardjo (2002:29), crime has been a social phenomenon since the beginning of human life on earth, but advances in communication technology have turned basic crimes into more complicated (modern) crimes. Traditional evil has been given a virtual (virtual) face in this way. Due to the intricacies of virtual crime or cybercrime, the general public, especially in a developing country with a digital divide like Indonesia, do not see it as a kind of crime. As a result of cybercrimes, countless victims (victims), as well as moral and financial losses. Members of the general public and netizens (dwellers of cyberspace/dwellers of cyberspace) can become victims.

Companies in business and ordinary individuals who do not have the expertise and knowledge of communication technology can fall victim to both. There is no need to go any further as we have all heard of cases involving "naked" students and artists that have been circulating on the internet. They become victims even though only a small percentage of them understand communication technology. Artists whose names begin with the letters YS, KD, KF, CK, and others are examples. That's just one example of a victim of cybercrime. However, others do not consider cyberporn to be a cybercrime. However, we have observed victims as a consequence of the hacker's actions. According to the Minister of State for Communication and Information, around 50% of young internet users prefer to visit pornographic sites (Kompas Cyber Media,

To understand cybercrime, one must first understand concepts such as hackers, crackers, and others. Because there are "black" and "white" characters, heroes and villains, just like there are in real life.

1) Hackers

"Hacker" literally means "cut or slice." They are generally individuals who use computers to attack computer networks (Republika, 22 August 1999). There is a similar definition in (2001:304), which states that a hacker is a subject matter expert. He knows how

to use a computer. He is quite computer savvy. Hackers are those who like to learn and tinker with computer systems. They are experts in hacking a company's communication network through cyberspace. Hackers adhere to Internet ethics or norms. They oppose censorship, deception, and coercion of the will of others. They assume that hacking is done in order to improve the security of an internet network. For example, if a bank claims that its network of communication systems is complex and impenetrable, making it impenetrable to everyone, hackers are encouraged to try, and if successful, they warn of how vulnerable the company's information systems are. As a result, many of them end up being hired by companies to secure information and communication networks in cyberspace.

2) Crackers

In the cyber world, there are hostile hackers. They are referred to as crackers. This cracker illegally infiltrates and destroys websites, websites, and internet network security systems for fun and profit. They are selfish and arrogant about their success in destroying company websites. His attacks were spectacular. The Pentagon's Department of Defense recorded 100 cracker attacks in a single day (Republika, January 6, 2000).

3) Carder

Carders are those who hack credit cards to obtain other people's card information and use it for personal gain. Victims often have a large number of credit cards. According to survey data, Indonesia is second after Ukraine in carding offenses in 2002.

4) Defacement

Defacement is the act of gaining access to a website and then changing its page appearance for a specific purpose. Blasphemers have targeted Indonesia, changed the TNI website. The hammer and sickle symbol replaces the Garuda Pancasila bird motif. On the website, there is now a picture of a naked woman.

5) Phreaker

A hacker is someone who gains unauthorized access to the telephone network to make free calls to any destination (Computeractive, No. 43/18 December 2002). Such incidents have occurred in Indonesian wartels.

Hackers are often educated people who have a certain level of formal education and can use or operate computers. are Crackers, people who are not technologically educated, financially incompetent, or from strata categorizing offenders into four groups (four).

1) Organizational work crimes

The culprit is the executive. They use the internet to commit crimes or harm others for their own or corporate gain.

2) Government work crime

The perpetrators are officials or bureaucrats who carry out criminal activities on the internet with the approval or direction of the state or government, but will reject charges if found.

3) Professional work crimes

Various jobs that include intentional criminal acts (malpractice).

4) Deviant individual work crime

Regardless of their social status, individuals may engage in business, capital ownership, or other self-help activities. These people choose deviant behavior in the workplace that violates the law or causes harm to others.

**Characteristics of "Cybercrime"**

**In many ways, cybercrime varies from conventional crime, including, but not limited to**:

1) Illegal, criminal, or immoral behavior occurs on the internet, making it difficult to determine which country's legal authority applies to them.
2) This exercise can be completed on any device that has an internet connection.
3) These actions cause monetary and immaterial losses (time, value, services, money, commodities, self-respect, dignity, and confidentiality of information) that are often greater than those caused by traditional criminal activities.
4) Offenders are those who have control over the use of the internet and its applications.
5) national dividing line

**"Cybercrime" in Indonesia**

Indonesia is a developing country lagging behind in the growth of modern communication technology. Indonesia's plan does not prioritize growth and technological excellence. After that, the transfer of knowledge from developed countries does not necessarily result in technical competence in developing countries such as Indonesia. Consider Malaysia, which has mass-produced software, computers and cell phones. Surprising, because Indonesia was the first Southeast Asian country to launch a communications satellite in the 1980s. Singapore and Malaysia, which at that time were still renting the Palapa satellite from Indonesia, grew into sophisticated countries with the latest communication technology.

Although still debated, Indonesia has a significant digital divide. The digital divide is the difference in access to communication technology between those who have and those who do not (Straubhaar & Larose, 2000:9). In addition to intellectual inequality and uneven economic growth in Indonesia, the ability to use communication technology is also not evenly distributed. Inequality can take many forms, including inequality, lack of information and telecommunications. Those who live closest to the community information center certainly have the best access.

Despite the digital divide, cybercrimes are common in Indonesia. Credit card theft by illegal hackers is the most common incident. They have the ability to use other people's credit cards to buy whatever they want, including gemstones, marine radar, business software, computer servers, Harley-Davidson motorcycles, and M-16 weapons (Warta Ekonomi.com, December 23, 2002). ). This is referred to as "carding." Carders (black hackers) use the internet to buy things and ship them back home. Ordered items can be used alone or sold at a lower cost. As an example,

a Sony laptop purchased through carding for 20 million rupiah was sold for 4 million rupiah. ClearCommerce, an internet security business based in Texas, rates Indonesia as one of the worst countries for crimes that take advantage of the complexities of communication

technology. In Indonesia, at least 20% of all credit card transactions made over the internet are fraudulent. The following data on internet related crimes are provided.

According to the statistics below (Koran Tempo, 26 March 2003), Yogyakarta is the leading city in Indonesia for cybercrime carding, with Bandung in second place. The atrocities were perpetrated by young people, the majority of whom were students. A student at a private university in Bandung once bought five Nokia Communicator cell phones and sold them for 5 million rupiah, even though the price at that time was around 10 million rupiah.

To avoid being caught, he hid in a nearby internet cafe, and when he received an order, he coordinated and paid an employee of a large parcel delivery bureau in Indonesia.

As a world leader in online credit card theft, Indonesia seems to be on the rise. Indonesia is often portrayed negatively, such as low per capita income, poor quality of education, and high levels of corruption, including carding in cybercrime.

Unexpected crime; it is indifferent to the place or context in which it occurs; it makes no comparison between perpetrator and victim; and does not take into account the caste or social position of the perpetrator or victim. When this happens, it may become an interesting topic for debate both in the media and in the lecture hall. This is especially true when crime is coupled with the complexity of communication technology. Even when we are not aware of it, the people around us are "innocent, as if without sin, and so delicate".

Apart from carding, defacement is a common type of cyber crime in Indonesia.

Black hackers have disrupted the appearance of websites on the Internet. Some examples (Raharjo, 202:35):

1) During the 1997 East Timor conflict, pro-Portuguese independence activists visited the websites of the Ministry of Foreign Affairs and ABRI (TNI, pen). They are also dangerous for commercial and educational sites. Attacks on crackers cause reactions from crackers. According to them, the cracker did it because he believed the attack was unfair and indiscriminate, regardless of whether it was a government-owned site, a business site, or an educational site.
2) In 1998, the front page of the Center for Scientific Information Documentation of the Indonesian Institute of Sciences (PDII LIPI) was replaced with a picture of a naked woman.
3) After the May 13-14 riots, Chinese crackers are said to have attacked the BKKBN, a government-owned facility. This episode occurred as a result of media coverage of the May riots in Indonesia, which resulted in ethnic Chinese individuals being killed and raped.
4) In June 1999, the POLRI website was updated with a nude image, followed by an image resembling the PDI-P emblem.
5) The Jakarta Stock Exchange (JSX), Bank Central Asia, and Indosatnet were all attacked in January 2000.
6) Fabian Clone, who had previously logged on to the Lippo Bank website, gained access to the Bank Bali website in September and October 2000. Despite the fact that both banks provide online banking, their losses are greater than those of the JSE.
7) In January 2001, a cracker targeted the website of PT. Ajinomoto Indonesia. This attack is a reaction to the enzyme porcine (pork), which is used as a catalyst in the production of spices.

Ajinomoto's website... http://www.mjk.ajinomoto.co.id When the prize is opened, a cheerful pig appears, as does the Pig line, opens on December 2K, "Ajinomoto You Are Lying to Us," and " Ajinomoto: HARAM HARAM... HARAM."

8) On 8 May 2001, the Indonesian Muslim Hacker Action Unit attacked the Polri website. (KAHMI). This happened in reaction to the arrest of the head of the Jihad Command Force.

Even if handled properly, the number of incidents and victims of cybercrime in the form of carding and defacement, as well as online pornography, can increase, although not everyone considers it a crime. However, it is possible that people close to us, such as our innocent wives and children, may use computer photo-engineering tools to broadcast their nude photos on the internet.

**The Urgency of Solving "Cybercrime" in Indonesia**

Given the large number of cybercrime incidents that have occurred and will certainly occur in the future, it is very important to deal with cybercrime issues as quickly as possible. The repressive and reactive techniques of law enforcement agencies are inadequate to deal with the changing and adapting criminal activity on the Internet. The officials were shocked. The rise in cybercrime highlights the government's inability to tackle it. As a consequence, the government must strengthen the expertise and experience of law enforcement officers in preventing, investigating and prosecuting cyber crimes. Cyber crime must be taken seriously by law enforcement.

Of course, this must be accompanied by a series of proactive and anticipatory actions taken by a number of major Indonesian institutions. In Indonesia, for example, agencies in charge of Internet Service Providers (ISPs) and internet cafes are mandated to take client protection measures.

The next step is to carry out extensive and sustainable marketing and education related to internet access to the wider community. If this is not done quickly, we can predict a statistically and qualitatively increase in the number of Internet crimes associated with the increase in Internet use in Indonesia. In the end, it will have a negative impact on Indonesia's internet industry and business. The world's online community, for example, may prohibit internet users with an Indonesian Internet Provider (IP) number from transacting online. As a result, all commercial activities on the internet will be completely eradicated.

Equally important, governments must move quickly to enact Cyberlaws to prevent cybercrime.

The previous economic system was questioned due to the inability of communication partners to meet face-to-face. To provide trust, it must be protected by cyberlaw. Despite the fact that internet users in Indonesia make up less than 5% of the total population (some estimates amount to 1.9 percent, or around 4.38 million), cyber law remains important as a legal framework for authorities fighting cyber crime. It would be even worse if the necessary legal mechanisms were not available.

**REFERENCES**

A. Book

Mahayana, Dimitri. 1999. Menjemput Masa Depan, Bandung: PT. Remaja Rosdakarya.

Naisbitt, John, Naisbitt, Nana, & Philips, Douglas. 2001. High Tech High Touch. Bandung: Mizan Pustaka.

Piliang, Yasraf Amir. 2001. Sebuah Dunia yang Menakutkan. Bandung: Mizan Pustaka.

Raharjo, Agus. 2002. Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi Tinggi. Bandung: Citra Aditya Bakti.

Straubhaar, J. & La Rose, R., Media Now, 2000.

Temporal, Paul, K.C. Lee. 2001. Hi-Tech Hi Touch Branding. Jakarta: Salemba Empat.

Ustadiyanto, Riyeke. 2001. Framework e-Commerce. Yogyakarta: Andi

Wilhelm, Anthony G, Demokrasi di Era Digital. 2003. Yogyakarta: Pustaka Pelajar.

A. Other Sources

Kompas Cyber Media, 05 Mei 2002.

Republika, 22 Agustus 1999.

komputer aktif, No. 43/18 Desember 2002.

Cybercrime_files\inline_files\SI10.HTM.

Warta Ekonomi.com, 23 Desember 2002.