Policies to Overcome the Increase in Cyber Crime in The Era of Globalization Realize Public Security

Nugraha Medica Prakasa

{nugrahamedicaprakasa84@gmail.com}

Universitas Lampung

Abstract. Policies to overcome the increase in cybercrime in the era of globalization are a very important effort in realizing community security. The rapid development of information and communication technology in the era of globalization has opened up new opportunities for criminals to commit criminal acts in cyberspace. Cybercrime has become a serious threat to the security of societies around the world. This study aims to analyze policies that can be used to overcome the increase in cybercrime in the era of globalization, focusing on efforts to realize community security. This research uses policy analysis methods to identify existing policies, analyze their effectiveness, and propose better policy recommendations. The problem that will be discussed in this study is how policies to overcome the increase in cybercrime in the era of globalization realize community security. The research method used is a normative research method with a statute approach and analyzed using content analysis.

Keywords: Law Enforcement, Cybercrime.

1 Introduction

Cybercrime or cybercrime is a crook act that uses PC innovation and web networks as its objective. Cybercrime itself emerges alongside the unremitting advanced innovation, data and correspondence that is developing. As a result of this event, numerous illegal and potentially harmful online activities have surfaced. With the rise of the wasteful idea of the local area during this pandemic, it opens up numerous open doors for cybercrime entertainers to do their activities. Many individuals utilize online locales for shopping, examining, working, and different things. Irresponsible people almost certainly use this to commit crimes. [1] Absence of public information about this can make it more straightforward for these people to perpetrate violations. The wrongdoing perpetrated is called cybercrim.

Types of *cybercrime* committed by cybercriminals include:

1) Data burglary is one type of unlawful activity by taking information from somebody through a PC framework or web network for individual use or promoted by selling taken information.
2) Hacking and Breaking can be deciphered as the demonstration of effectively breaking into programs contained in other gatherings' PCs. A programmer shouldn't

MIC 2023, October 28, Jakarta, Indonesia

DOI 10.4108/eai.28-10-2023.2341686

make a terrible difference, on the grounds that at times there are hacking activities that make a positive difference. Notwithstanding, hacking abilities are frequently abused by programmers to acquire individual advantages that hurt others.

3) Dissemination of Unlawful Substance is a demonstration that spreads content that contains data and information that isn't be guaranteed to valid, unscrupulous and abuses the law.

4) Carding or otherwise called Visa misuse is a shopping movement yet utilizes the number and character of a charge card claimed by another person.[2]

The rising number of cybercrimes or cybercrimes we as a general public should be more cautious in getting to the web, particularly regarding shopping and furthermore sharing our own data in any spot. To act as an illustration of the case, one of the most recent and stunning programmer activities is the situation of information robbery of 15 million Tokopedia account data which is accounted for to have been effectively penetrated. There are eyewitnesses who even say, a sum of 91 million records of the internet based store monster have been attempted to sell on the dull web for US $ 5,000. The degree of the reality of this data is as yet being followed by the specialists. There are a lot of people who fall prey to scams and cybercriminals who take advantage of people's lack of knowledge about how to protect their personal identities when using information technology. Individual characters that ought to simply be known to banking organizations, are unwittingly given to obscure unfamiliar gatherings. Consequently, it is inclined to being utilized by untrustworthy gatherings to get to their monetary condition.[3]

For this situation, there are three ways to deal with keeping up with security in the internet, the first is the mechanical methodology, the second is the socio-social moral methodology, and the third is the lawful methodology. To conquer the security of obstruction, the innovative methodology is totally important, in light of the fact that without an organization security it will be extremely simple to be compromised, or got to wrongfully and without privileges. Viewing at the legitimate realities as they exist today, the effect of the improvement of science and innovation that has been abused for the purpose of wrongdoing is vital to guess how the legitimate approach is, so cybercrime that happens can be countered with criminal regulation, remembering for this case the confirmation framework. It is supposed to be vital on the grounds that in the requirement of criminal regulation the premise of defense for an individual can be supposed to be liable or not of carrying out a crook act, notwithstanding his activities can be faulted for the strength of prior regulations (the guideline of lawfulness), likewise which activities are upheld by the strength of substantial proof and can be represented (component of responsibility). Aside from that, a very important question to discuss is who should take preventative measures when carrying out law enforcement if the cybercriminals are minors.[4]

The fast improvement of innovation requires legitimate game plans connected with the utilization of innovation. Many cases demonstrate that legitimate instruments in the IT field are as yet frail, this should be visible from juridical requirements and non-juridical limitations. The juridical impediment is that electronic reports are as yet not explicitly perceived as proof by the Criminal Method Code and in court guidelines. The trouble of recognizing these violations, prompted by the absence of sufficient hardware, the hesitance of certain casualties to answer to the police, the security arrangement of the proprietor of resources/frameworks that are moderately feeble, challenging to follow the whereabouts/home of the culprits of wrongdoings. It turns out that there is currently no item in our nation that can be used to trap cybercriminals. For checking cases, for instance, the police can accuse PC hoodlums of Article 363 of the Crook Code about burglary on the grounds that the suspect took others' charge card information. This is the foundation why it is important to look for the job or activity of the public authority both

preventively and abusively in managing the issue of cybercrime which is expanding in number, generally the local area will have a real sense of reassurance and agreeable. In view of the foundation portrayal over, the issue in this study is the means by which the issue of beating the expansion in cybercrime in the time of globalization acknowledges local area security.

2 Research Methods

The exploration strategy utilized is a regularizing research technique. By utilizing resolution approach connected with the issue of defeating the expansion in cybercrime in the period of globalization, acknowledging local area security.[5] The resolution approach is to analyze matters concerning legitimate standards, lawful perspectives and tenets, and regulations and guidelines connected with the climate, and exact and responsible information connected with the issue of conquering the expansion in cybercrime in the period of globalization to acknowledge local area security. Furthermore, a top to bottom assessment of the lawful realities is additionally held to then look for answers for the issues that emerge in the side effects concerned. [6]

3 Results and Discussion

Mechanical improvements in Indonesia. In accordance with the improvement cycle and the period of globalization, as well as the rising nature of innovation, Indonesian culture has encountered many changes because of the present advances in Science and Innovation. Individuals' reasoning has additionally been affected by different things. The effect caused can be as sure effects or adverse consequences.[7] The positive effect gives accommodation to the local area in finishing their exercises, while the adverse consequence can be as disintegration in open confidence, with the limitless section of unfamiliar societies through web-based media, the ascent of erotic entertainment that causes inappropriate behavior, internet betting, cybercrime, and what has as of late been overflowing is the act of online prostitution business through interpersonal organizations or different destinations. Likewise, there are additionally adverse consequences that emerge with the web. Web can likewise be utilized for negative things and mischief to other people, for example, charge card burglary, robbery or site annihilation. The introduction of Regulation Number 11 of 2008 concerning Electronic Data and Exchanges (ITE) is planned to give many advantages, including to guarantee lawful assurance for individuals who go through with electronic exchanges, support financial development, forestall data innovation based wrongdoings and safeguard administration clients by using data innovation. [8]

In Indonesia, cybercrime is really not another wrongdoing. Cybercrimes a term that alludes to crime by utilizing PCs or PC networks as instruments, or as focuses, as well as, areas of wrongdoing. In an ideal world, this would not be the case, and it is difficult for people to become cybercriminals' victims. However, in Indonesia, assurances and endeavors to safeguard general society from becoming casualties of cybercriminal misuse rehearses are frequently difficult. Many cases demonstrate that individuals are casualties of fake pernicious acts of cybercrime entertainers who exploit the second when the interest for clinical gadgets, for example, covers and hand sanitizers take off strongly. Individuals who attempt to purchase covers or hand sanitizers through deals destinations in the internet, frequently become survivors of untrustworthy individuals.

Certain individuals who have previously purchased merchandise by means of on the web and have moved some cash, evidently get undesirable things. The things they requested were never conveyed, as a matter of fact. Second, because of public obliviousness about the significance of keeping up with the secrecy of their records and individual personality, certain individuals become survivors of misrepresentation perpetrated by cybercriminals. False messages, SMS, messages via web-based entertainment requesting thing request codes, Visa numbers, PIN numbers, and so forth., frequently minus any additional confirmation are addressed guiltlessly. Despite the fact that it is extremely dangerous. Individuals who live in the period of credit only economy, some don't know about the dangers and risks of making on the web exchanges, yet frequently get found out in the draw of prizes. Grandiosity and different other fake practices are created by cybercriminals. Anything the circumstance, people in general ought to know and careful about friendly designing and phishing that are normally evolved by cybercriminals to trick their prey. Individuals who live or work at home, and depend additional on data from online sources, for example, email and talk, are generally bound to be utilized by programmers to take significant information and data with phishing techniques. With something that seems urgent, con artists play tricks on people's minds.

3.1 Problems in Countering the Increase in *Cyber Crime*

The danger of cybercrime in Indonesia is a wrongdoing in the period of an undeniably stressing computerized society. In the Condition of the Web report in2013, for instance, Indonesia was referenced as the country with the second spot in cybercrime cases on the planet. The quantity of cybercrimes in Indonesia that year was accounted for to arrive at 36.6 million assaults. Something other than insurance and preventive estimates that depend on crafted by the Public Digital Organization and Correspondence and Data, endeavors to shield people in general from becoming survivors of cybercrime positively likewise rely upon the capacity and data education of the local area itself. Train individuals' awareness and basic disposition so as not to open email and connections that are dubious or come from untrusted sources. Continuously be careful about any electronic records appended. Since, it can contain unsafe substance, which are things that ought to be consequently finished by individuals who know and have satisfactory data education.

The use of information technology and the internet has soared rapidly in recent decades. While this brings great benefits in our lives, it also presents a new threat in the form of increased *cybercrime*. *Cyber*crimes a crime committed through digital media with the aim of stealing personal information, damaging computer systems, or even threatening state security. The problem of tackling the increase in *cybercrime* is a very important challenge in this increasingly connected world.

a) Technological Advancement: One of the main problems in tackling cybercrime is the rapid development of technology. Cybercriminals are always looking for loopholes in new systems, so law enforcement efforts often fall behind. Sustainability in security technology updates is essential, but often expensive and difficult to do.
b) International Nature of *Cyber Crime*: Cybercrime is not limited by national borders. Perpetrators can operate from any country, so national law enforcement is often ineffective. International coordination and cooperation are key in pursuing and punishing perpetrators *of cybercrime*.
c) Indifference and Ignorance: The general public is often unaware of the potential threat of cybercrime or less concerned about cybersecurity. This can make them vulnerable to attack. Education and increased digital awareness are essential to address this issue.

d) Lack of Resources: Many countries, especially developing ones, face the problem of lack of human and financial resources in *countering cybercrime*. This has resulted in a lack of ability to develop capable law enforcement teams and adequate cybersecurity infrastructure.
e) Legal Challenges: Applicable laws often cannot keep up with technology quickly. This can result in difficulties in prosecuting *cybercrime* perpetrators, especially if the case involves national borders.
f) Privacy and Security: Cybercrime law enforcement often sparks debate about the extent to which governments may violate individual privacy in the interest of security. This becomes a complex ethical and legal dilemma.
g) The Evolution of Perpetrator Tactics: *Cybercriminals* are constantly evolving their tactics and techniques, making it difficult to catch up to them. This requires ongoing efforts in cybersecurity research and development.

Despite this issue, states, policing, organizations, and networks should cooperate to make a more secure environment in the digital world. Expanded mindfulness, interest in security innovation, close worldwide collaboration, and upgrades in the legitimate system are a portion of the means that can be taken to address the ascent in cybercrime. With better worldwide collaboration and more noteworthy regard for this issue, we can expect to diminish the staggering effect of cybercrime and protect us. In light of this, the issue that emerges according to cybercrime is the way to kill or implement the law. The fast improvement of innovation requires lawful game plans connected with the utilization of these advancements. Tragically, as of not long ago numerous nations (counting Indonesia) don't have explicit regulation in that frame of mind of data innovation, both in criminal and common angles. The slacking regulation in adjusting to progresses in data innovation requests a transitory answer for defeat cybercrime, in particular through leading edge court choices. Many cases demonstrate that legitimate devices in the IT field are as yet powerless. For instance, electronic archives are as yet not explicitly perceived as proof by the Criminal Method Code. It tends to be found in Regulation No. 8/1991 Article 184 section 1 that this Regulation authoritatively restricts proof to observe articulations, master explanations, letters, directions, and proclamations of the charged as it were.

Besides, notwithstanding lawful instruments, unique foundations, both government-claimed and NGO (non-government associations), are required as a work to battle wrongdoing on the web. For instance, the US has the PC Wrongdoing and Licensed innovation Segment (CCIPS) as a unique division of the U.S. Division of Equity. This organization gives data about cybercrime, conducts escalated socialization to the local area, and behaviors exceptional examination in battling cybercrime. There is likewise the Public Framework Security Center (NIPC) as an organization in the US that handles foundation related issues. This foundation recognizes basic pieces of framework for the country (particularly for the US.[9] The internet, also known as the computer network, is already regarded as an infrastructure that requires particular care. This organization likewise gives warning to every individual who needs an answer for violations in the PC field.

Issues connected with cybercrime in the event that not completed oversight or policing, then, at that point, in any time this wrongdoing will keep on expanding. Consequently, an activity or job of the public authority is expected to do management both preventively and harshly focused on legitimate change and public security in the period of globalization and high level mechanical improvements as it is today. This is on the grounds that today, particularly in Indonesia, the utilization of innovation based media has been generally utilized, subsequently it

is important to intently screen cybercrime so it doesn't proceed to increment and the hurt local area isn't expanding.

3.2 The Urgency of Legal Policy and Legal Reform in Overcoming the Problem of *Cyber Crime*

Mechanical advances have suggestions for the improvement of wrongdoing. Using the internet and other electronic devices, traditional crimes are now being transformed into cybercrimes. Cybercriminals have access to the internet, which enables them to carry out their crimes in a manner that is more neatly organized, concealed, and able to penetrate both space and time in a very broad range. As a type of globalization of wrongdoing, cybercrime can be completed by including a few culprits situated in a few purviews of various nations with target casualties situated in different nations too. Wrongdoings carried out in the internet by and large plan to create monetary advantages for the culprits. Different activities are completed to go after security frameworks in the internet to bring in cash. There are likewise culprits who utilize the web as a medium to bring in cash, for instance the utilization of the web for illegal dealing with weapons and organs, prostitution and erotic entertainment. In its turn of events, lawbreakers use web media as a way to go after somebody by and by without straightforwardly or for sure not going for the gold, like slander through the web, political hacking, digital psychological oppression, digital harassing, etc.

Indonesia has gone under more prominent examination from cybercrime experts lately, particularly since a 2013 review by Akamai Innovations, IT security firm, detailed that Indonesia has surpassed China as the world's biggest wellspring of hacking traffic. The information doesn't exclusively imply that the culprits come from Indonesia, yet as of not long ago issues connected with cybercrime, keep on expanding in addition to with the presence of Coronavirus which movements of every kind should be done at home utilizing electronic media, it requires the public authority to fortify guidelines to manage cybercrime issues. Moreover, issues connected with cybercrime are connected with:

a. The attributes of cybercrime propose that these violations can cross state locales, while the presence of peaceful accords on policing cybercrime is still extremely restricted.

b. Penal arrangements in battling cybercrime have not been offset with non-correctional approaches like strategies in the workplace, strategies in applications, approaches in schools, etc.

c. Law authorization should manage billions of netizens (web clients) with different web ways of behaving. Combating cybercrime is difficult due to inadequate law enforcement resources.

In this manner, cooperative energy is required between the public authority and confidential gatherings and different nations in managing cybercrime with the goal that the number doesn't keep on expanding. Because it is an urgent matter, or the urgency of legal reform related to cybercrime that can be done with criminal law politics to deal with this problem, this is related to tackling cybercrime must take precedence over legal reform.

Criminal arrangement is utilized as an option in finishing social approach. Beating social issues is done by policing is a reaction to wrongdoings carried out by the local area. As a reaction to wrongdoing, the criminal strategy has restrictions in handling violations that are so expansive

and complex, hence wrongdoing decrease is done by correctional means (the utilization of criminal regulation) and offset with non-reformatory means. Cybercrimes one of the results of the globalization of wrongdoing, where violations are perpetrated without being restricted to existence. Muladi and Diah Sulistyani R.S. made sense of that the speed increase of present day transportation, correspondence and data brought forth innovative globalization which influences the globalization of wrongdoing. Moreover, criminal strategy that should be possible in conquering this is by war making criminal science or mischief making on wrongdoing that is unfriendly (adversarialism) as a harsh methodology and joined with a preventive methodology mutualism or harmony based on peacemaking criminal science. In handling cybercrime, complete endeavors are required both through criminal regulation and through criminal regulation channels. Wrongdoing avoidance and control is completed with a fundamental methodology between correctional arrangement and non-punishment strategy. Correctional arrangement has a few constraints and shortcomings, to be specific zero down to earth, individualistic (guilty party situated), more oppressive and should be upheld by framework that requires significant expenses. Along these lines, wrongdoing avoidance is better done utilizing non-correctional strategies that are preventive. Strategies in fighting cybercrime should be possible with two occasions, to be specific:

a. Penal Policy

Corrective strategy is an arrangement connected with the utilization of criminal approvals in tackling wrongdoing cases in the internet. This is connected with cybercrime policing, implementation is completed to meet the worth of equity, particularly for casualties. The worth of equity possesses a crucial and fundamental component in the development, application and implementation of regulations. The worth of equity is an outright necessity in the existence of society, country and state as per the standards of the Pancasila regulation.

b. Non-Penal Policy (Role of the Prosecutor)

Non-penal policies that can be done are as follows:

1) Develop arrangements outside the criminal regulation that help cybercrime counteraction endeavors, like through enemy of disdain approaches, hostile to harassing strategies and solid web approaches through the schooling system;

2) Socializing likely wrongdoings in the internet by teaching the web client local area not to incorporate individual character, executing in places with secure web offices, etc;

3) Building participation with the confidential area to fabricate a security framework in the internet;

4) To combat cybercrime on a national and international scale, establish institutional networks. Global collaboration in countering cybercrimes exceptionally important thinking about that cybercrimes a transnational coordinated wrongdoing.

As an emerging nation, Indonesia should be quick in acclimating to legitimate turns of events and methodologies in handling cybercrime. The development of a global strategy for the prevention and enforcement of law against cybercrime, the development of responsive legal formulations, and the preparation of institutions that can take swift action when problems arise in cyberspace are the means by which legal politics in the fight against cybercrime is carried out. Lawful change is a work to additionally improve and consummate legitimate direction connected with cybercrime. This work is done by improving the codification and unification of regulation, in execution should focus on lawful mindfulness creates in the public arena. This is

more accentuated in the circumstance that keeps on creating, the law will keep on staying aware of the times. For this situation, the advancement of the times in the area of innovation that can cause criminal demonstrations, thusly it is important to organize and shape regulations that are more responsive in managing cybercrime issues.

4 Conclusion

Based on the results of research related to policies to overcome the increase in *cybercrime* in the era of globalization, it is known that the increase in *cybercrime* in the era of globalization requires a holistic approach involving the government, the private sector, and the general public. Some policies that can be adopted include increasing penalties for cybercrime perpetrators, increasing digital awareness and literacy in the community, international cooperation in cybercrime law enforcement, and developing more sophisticated cyber security technology. In tackling *cybercrime*, thorough endeavors are required both through criminal regulation and through criminal regulation channels. Wrongdoing avoidance and control is completed with a fundamental methodology between correctional arrangement and non-punishment strategy. Correctional arrangement has a few constraints and shortcomings, to be specific zero down to earth, individualistic (guilty party situated), more oppressive and should be upheld by framework that requires significant expenses. Subsequently, wrongdoing counteraction is better done utilizing non-punitive strategies that are preventive.

References

[1] S. Karyadi dan S. Suparno, "Juridical Overview of the Crime of Terrorism in Indonesia," dalam *Proceedings of the First Multidiscipline International Conference, MIC 2021, October 30 2021, Jakarta, Indonesia*, Jakarta, Indonesia: EAI, 2022. doi: 10.4108/eai.30-10-2021.2315770.

[2] L. Ferdiles dan A. Budianto, "A Judicial Review of the Application Restorative Justice Principle in Efforts to Resolve Criminal Acts Who Committed by Childs Law," dalam *Proceedings of the First Multidiscipline International Conference, MIC 2021, October 30 2021, Jakarta, Indonesia*, Jakarta, Indonesia: EAI, 2022. doi: 10.4108/eai.30-10-2021.2315785.

[3] Y. Rizal dan Z. Fakrulloh, "Application of Ultimum Remedium Principle in Tax Criminal Law," dalam *Proceedings of the First Multidiscipline International Conference, MIC 2021, October 30 2021, Jakarta, Indonesia*, Jakarta, Indonesia: EAI, 2022. doi: 10.4108/eai.30-10-2021.2315853.

[4] R. Listio dan Z. Fakrulloh, "Law Enforcement in the Implementation of Law Number 40 of 2014 concerning Insurance Against the Impact of the Covid-19 Pandemic for the Indonesian Insurance Society," dalam *Proceedings of the First Multidiscipline International Conference, MIC 2021, October 30 2021, Jakarta, Indonesia*, Jakarta, Indonesia: EAI, 2022. doi: 10.4108/eai.30-10-2021.2315670.

[5] Ali Zainuddin, *Metode Penelitian Hukum*. Jakarta: Sinar Grafika, 2011.

[6] Ashsofa, Burhan, *Metode Penelitan Hukum*. Jakarta: Rineka Cipta, 2007.

[7] E. Riswanto dan R. Riswadi, "Judicial Review of the Law on Community Organisations in Indonesia," dalam *Proceedings of the First Multidiscipline International Conference, MIC 2021, October 30 2021, Jakarta, Indonesia*, Jakarta, Indonesia: EAI, 2022. doi: 10.4108/eai.30-10-2021.2315814.

[8] R. Saka, F. Santiago, dan M. Barthos, "Juridical Review of Good Corporate Governance Principle in Law Number 40 of 2007 Concerning Limited Liability Company," dalam *Proceedings of the 2nd Multidisciplinary International Conference, MIC 2022, 12 November 2022, Semarang, Central Java, Indonesia*, Semarang, Indonesia: EAI, 2023. doi: 10.4108/eai.12-11-2022.2327288.

[9] Irianto, Sigit, "Kedudukan yang Sama di Depan Hukum (Equality before the Law) dalam Penegakan Hukum di Indonesia," *Jurnal Hukum dan Dinamika Masyarakat*, vol. 5, no. 2, hlm. 2010.