Journal Equity of Law and Governance

Vol. 4, No. 1
ISSN: 2775-9512 (Print) 2776-5121 (Online)
https://www.ejournal.warmadewa.ac.id/index.php/elg

Critical Analysis of The Republic of Indonesia Police in The Implementation of Cybercrime Law in Indonesia

Yaris Adhial Fajrin[1]*, Muh. Fadli Faisal Rasyid[2], Grenaldo Ginting[3], Eka Ari Endrawati[4], Viorizza Suciani Putri[5]

[1*]*Faculty of Law, Muhammadiyah Malang University, Malang, Indonesia*
yaris@umm.ac.id
[2]*Faculty of Law, Andi Sapada Institute of Social Sciences and Business, Parepare, Indonesia*
fadlifaisal643@gmail.com
[3]*Faculty of Law, Indonesian Christian University Tomohon, Indonesia*
grenaldoginting@gmail.com
[4]*Faculty of Engineering, Krisnadwipayana University, Jakarta, Indonesia*
ekawati@unkris.ac.id
[5]*Supreme of Court Republic Indonesia*
viorizza@mahkamahagung.go,id

Abstract - The purpose of this research, which is based on an evaluation of Indonesia's cybercrime legislation, is to examine the difficulties encountered by the Indonesian National Police in carrying out their duties to combat cybercrime and computer crime, and to draw conclusions about how recent technological advancements have contributed to an increase in both the frequency and severity of these crimes. This study employs a philosophical and analytical approach to normative law as its research methodology. It examines applicable statutes and regulations, as well as legal theory and current practices in law enforcement. Cybercrime is on the rise, and the study's findings suggest that this trend is directly tied to the expansion of information technology, which in turn allows cybercriminals to employ more complex strategies. Not having clear legislative restrictions pertaining to cybercrime, insufficient preparation on the part of law enforcement, subpar system security, and an uninformed public are the primary challenges. Some of the proposals include creating communication platforms amongst law enforcement agencies to boost collaboration in the fight against cybercrime, educating the public and conducting targeted investigations using cutting-edge technical methods, and expanding outreach and education efforts to the general population.

Keywords: Cybercrime, Law Enforcement, Indonesian Republic Police

I. INTRODUCTION

In common parlance, "cyber crime" is any criminal conduct in which a computer or network is either directly or indirectly involved (Puluhulawa dkk., 2023). Cybercrime includes things like child pornography, online auction fraud, forgery checks, credit card fraud, trust fraud, identity fraud, and more. Cybercrime is usually defined as any illegal action involving a computer or a computer network. However, the term is also used for more common types of crime where computers or computer networks are used to help or make the crime possible (Shah dkk., 2022). So much technological progress has been made so quickly. Modern technology has come a long way in a very short amount of time. The people who make technology are confused about how to handle it because it moves so quickly. You could even say that technology is giving up on managing people. We are part of a change that is already under way. Like other uprisings, this one brings about quick changes that often overturn long-held beliefs and ways of doing things (Bunga, 2019).

One important thing about this change, which is getting stronger and has never happened before in human history, is its speed. A race was going on to cut down on the distance, and people were trying to take over space and time (Mohammed dkk., 2019). The change we are living through is the IT revolution. When computers were first invented, they set off the IT revolution. Since then, computers have created their own world, which is now known as cyberspace or virtually nature. Actually, the way websites talk to each other or the way groups talk to each other in IT has turned into its own big subsystem, which looks like a small world. The information society is thought to be one of the most important goals of world society in the third millennium. One thing that makes it clear is that people in both developed and developing countries are using the internet more and more for almost every task in their lives. Indonesia is one of these growing countries.

Because of this, "information" has become a very valuable and successful good in the market. The United States, which was one of the first countries to use the internet, has switched from a manufacturing-based economy to a service-based economy in response to this change. The old legal materials are becoming less important, while the legal materials of a service-based economy, like information in the American economy, are becoming more important (Oni dkk., 2019). Because the internet doesn't care about physical borders and works entirely online, it also creates new activities that can't be fully controlled by current laws. The public is now more aware of the need for rules to govern activities that happen on the internet because of this.

A lot of good things can come from having the internet, but it also brings about new worries. For example, cyber crime, which includes the rise of sexual sites and attacks on people's privacy, is a new type of crime that is more complex. As it has grown, it has become clear that using the internet can be bad because it makes it easier for bad behaviour and crimes to happen that were thought to be impossible before. "Crime is a product of society itself," says one idea..(Mohsin, 2021)

Besides the crime that happens in internet, this new world has also brought about a number of new cultures that are important to the police. For example, emails, which are short for "electronic mail," have their own addresses. More and more people are writing letters through email instead of regular mail because it is more convenient, cheaper, faster, safer, and can be sent and received from anywhere. In this way, the way people can get to each other now also needs to take these traditional forms into account. In this case, it's possible that important witnesses who want to stay private will only give information online.

Following what was said in the opening, the problem that can be put forward is: (1) What changes have you seen in computer crime and online crime in Indonesia? and (2) In what ways does it get hard for the Indonesian National Police to enforce the law against cybercrime and computer crime?, based on the research formulation, So it can be concluded that the research objectives are as follows: To assess and document the changes observed in computer crime and online crime within the context of Indonesia, including trends, patterns, and emerging challenges and To identify and analyze the specific obstacles and challenges encountered by the Indonesian National Police in effectively enforcing cybercrime and computer crime laws, with a focus on understanding the legal, technological, institutional, and societal factors contributing to these difficulties.

II. METHOD

This study is categorized as normative legal research because it is based on the issue or theme raised as a research topic. Normative legal research, underpinned by a philosophical and analytical approach, offers a robust framework for critically examining the implementation of cybercrime law by the Indonesian police. The research approach used is philosophical and analytical, namely research that focuses on rational views, critical and philosophical analysis, and ends with conclusions that aim to produce new findings as an answer to the main problem that has been set (Ishaq, 2017). Will be analyzed with descriptive analytical methods, namely

by describing the applicable legislation related to the theory of law and positive law enforcement practices related to the problem (Mahmud Marzuki, 2005).

III. RESULT AND DISCUSSION

When it comes to how the terms computer crime and cyber crime are used and what they mean, there is a difference between the two. The first point of view says that the two types of crime are the same. While the second view says that the two types of crime are different based on the way they are committed and the means they use (Givens, 2023).

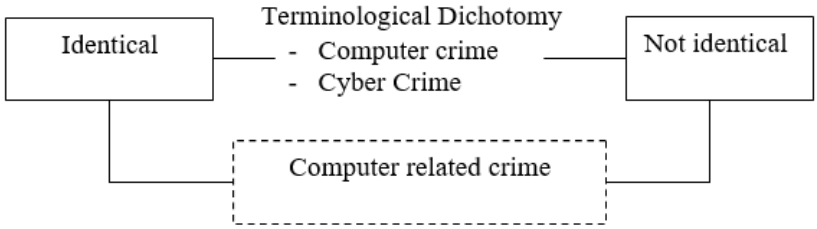

Figure 1 Dichotomy Scheme of Computer Crime and Cyber Crime

According to the US Department of Justice, computer crime is "any illegal act that requires knowledge of computer technology for its commission, investigation, or prosecution." This is how computer crime is different from cyber crime. "Any illegal, unethical, or unauthorised behaviour relating to the automatic processing and/or transmission of data" is another way the Organisation for European Community Development sees it. He wrote a book called Criminal Aspects in the Computer Sector, in which he says, "crime in the computer sector can generally be interpreted as illegal use of computers." Combining the above meanings, we can say that a computer crime is any illegal act done with a computer as a tool or an object, whether the goal is to make money or hurt other people. To sum up, a computer crime is an illegal act that is done with advanced computer technology. Cyber crime, on the other hand, is any action or behaviour that goes against the law, is unethical, or isn't allowed when it comes to processing and/or sending data. Most of the time, these things are done on or with computers or other digital tools in a virtual world (cyber). By comparing the two meanings' conclusions, we can see that the definition of computer crime given above is the same as the definition given for cyber crime. The only thing that these two types of crime have in common is that the person involved is illegal, no matter what network method is used.

Nazura Abdul Manap has the second view, which says that computer crime and cyber crime are different depending on the mode and media used. She says, "Broadly defined, computer crime can cover a wide range of different things. violations, criminal activities or issues." One who does this has a direct connection with the computer and is breaking the law by using a computer as a tool. For example, a dishonest bank worker who moves customer money to a sleeping account for his own gain, or someone who directly accesses someone else's computer to download important data without their permission. In this case, the hacker needs to be able to directly enter the victim's computer. It doesn't use the internet or only a small network like a LAN. Cyber crime, on the other hand, is a crime that is done virtually over the internet. That is, the acts that were done can spread to other countries that are not governed by that country. In this second meaning, it's clear that direct relationships and the use of a network system that separates the mode and media at the time of the crime are necessary.

Recent changes in how computers are used and how they connect to the internet have led to a trend of passive business growth and greater competition in world trade. There aren't many costs associated with using the internet to promote, sell, service, and carry out online transactions. It has also been shown to help the global business market grow. This is what

drives business leaders to improve internet media in the hopes of making more money all the time. There is a lot of activity in the online world as a business tool, but at the same time, new types of business and economic crime are growing and using the internet to do their work. As of right now, there isn't a single agreed upon meaning of either "economic crime" or "business crime." However, the definition below can be used as a starting point. Criminal acts done for financial reasons are called economic crimes or business crimes.

After looking at a lot of old books and studies, it's clear that economic crime in the cyber world has grown in a straight line as more media and technology are used in the cyber world for global business and trade. Take a look at how traditional trade between countries has changed into electronic commerce (e-commerce), how businesses are becoming more aware of the need to protect intangible assets like intellectual property, and how the cyber world is used for things like online banking and virtual (online) business dispute resolution. Because VoIP, e-mail, and chat make it easy for businesses and traders to talk to each other, there has been an increase in business crimes that involve misusing the internet. Business crimes include frauds in bankruptcy, bribes, embezzlement, and theft. False claims against the government, violations of food, drug, and cosmetic laws, securities laws, monopolies, and antitrust laws are some examples of acts that can be put into this category (Sari, 2023).

Tubagus Ronny Rahman Nitibaskara says that if the current rules are used to handle online crime cases, then they will be different from how law enforcement works in the real world, especially when it comes to what police officers have to do. You don't need a gun or a stick to do your job; you just need to be good at using technology. In line with Soerjono Soekanto's thoughts on the things that affect law enforcement, in order to fight online crime (Fahmi, 2014):

a. There are rules
b. There is an institution that will enforce the rules
c. The existence of facilities that support the implementation of regulations
d. There is legal awareness among the people affected by this regulation.

So these four factors need to be seen with a new paradigm, namely the cyber paradigm. The way that crime will go is hard to guess, according to Fattah, because there are so many factors that can cause it. So that how crimes are dealt with becomes uncertain and controversial. Andi Hamzah, on the other hand, says that crimes should be illegal no matter what the ideology, interests, or outlook of a country is. For example, computer crimes should be dealt with by criminal law. At the same time, Jan Smits says that the world of law doesn't see the problem of technological progress. The goal for lawyers isn't to get better at using technology (Rahman dkk., 2024). They don't need to learn how to use the tools; what they need is information about criminal law. To deal with violations, legal experts focus on the question of what steps need to be taken.

Development of computer crime and cyber crime in Indonesia.

In the last chapter, it was said that all of the definitions or limits given about computer crime, computer misuse, and cyber crime can be summed up as actions or behaviours that use a computer as a tool or means to commit a crime, or even the computer itself becomes the victim of a crime. So, the view on the two types of computer crimes has a small and a broad range of possibilities.

Computer crime, in a narrow sense, is any illegal act done with advanced computer technology. Also, in a broad sense, computer crime is any illegal activity that includes not only advanced computer technology but also a worldwide network of information and electronic devices, both computer-based and not, that can connect to the network and carry out the illegal activity. If we use this meaning, we can see the history of computer crime and cyber crime not as a collection of separate events, but as a series that shows how far it has come.

Comparative indicators are also needed to find an object observed in study in order to figure out how it has changed over time. In order to study the history of computer crime and cyber crime, researchers not only look at how people used information technology in the early stages of its development until a new type of computer crime and cyber crime appeared, but

they also look at how crimes are spread around the world by using world applications. crime done by hackers every once in a while. What does the name mean? The way people think about reporting this kind of crime changes linearly as computer technology and innovations in the online world itself change.

If you look at the table above that shows how computer technology has changed from one generation to the next, you can see that it has sometimes gotten better in terms of using less hardware, making applications that focus on the user more, getting smaller, and making access faster. lighter and faster, with more memory space, programming features that are getting smarter, and products that have been proven to last. There is also evidence that, in addition to hardware that keeps getting better, different software programmes that help people use computers can also keep up with new technologies (Tanjung & Adriani, 2022). So currently there are various applications ranging from standard office-style typing and calculation programs, to complex three-dimensional animation engineering applications and arithmetic statistical analysis that are very easy to use

When each part of a computer technology product is linked to the internet, a global information and communication network, they work together in many ways that are beneficial. To be more specific, the internet has gone through an amazing process of changing itself. Experts and observers in information technology (IT) say that the internet is now in its second age. People who live in these kinds of situations can do both good and bad things. For example, they can expand business transactions and trade in cyberspace, which we call e-commerce. On the other hand, criminals can use these conditions to do a wide range of illegal activities. The chart below shows how the first generation of the internet is different from the second generation of the internet and how they are alike.

The growth of computer crime and online crime shows how complicated they are, both in terms of the types of crimes and the amounts that happen. It was discovered that some types of computer crime and cyber crime that were only done in the real world are now also done in the virtual world. For example, scams and threats made through the internet have spread. A lot of new types of crime have also started to happen on the second-generation internet that weren't common in the early days of using computers on the first-generation internet. This is because they need systems that are only available on the second-generation internet, like web traps, carding, defacement, etc. Additionally, it seems that online crime makes use of modern technology to carry out its activities (Antoni, 2017). People who have this trait need to know about and always be on top of new changes in the world of information technology. This is what makes it different from other common crimes.

As technology, mostly computers and phone networks, has grown, so has the range of crimes that happen with it. These crimes now include business activities that happen in internet. It can be seen that crime in the business world that uses cyber facilities started to rise when people started using new ways to trade over the internet, like e-commerce (or electronic commerce), where they could trade information and data without having to meet in person. People first used electronic commerce (E-commerce) to buy and sell things, like CDs and books, through websites on the internet (www) (Siburian, 2016). But e-commerce has come a long way and now includes a lot of activities in the banking and insurance services sector. For example, you can use it to check your account balance, apply for a loan and more. E-commerce hasn't been defined in a single way yet, and it looks like it's one of the things that is growing very quickly and strongly in cyberspace.

With a few words, e-commerce means buying and selling things and services over the internet. When it comes to how it works, e-commerce can be either B to B (business to business) or B to C (business to customer). For the last one (B to C), consumers need to be extra careful because their stance is usually not as strong as the company's. This can lead to a number of issues, so consumers should be careful when they buy things online. Among these problems are payment methods and security guarantees in transactions (security risk), as well as personal security guarantees in e-commerce in general when it comes to the transfer of information like credit card data and personal consumer data.

In the years that followed, crimes that happened online started to affect more than just e-commerce deals and apps. They also started to affect different parts of trading in cyberspace. One well-known problem is business crime, which involves people's intellectual property rights and has to do with business. Ofense against intellectual property is the name of this crime. You can be charged with this crime if you use someone else's intellectual property rights on the internet. illegally copying the look of a web page on someone else's site, for example, or posting information on the internet that turns out to be someone else's trade secret, and so on. Software theft, which has become popular these days, is another type that is just as bad. People who make software can lose money because their work can be stolen by getting it from the internet and burning it to a CD. This work is then copied illegally without the creator's or royalty holder's permission.

Recently, credit card fraud, stock exchange fraud, banking fraud, child pornography, and drug trafficking have also become very popular. These are just a few examples of how crime is changing in the business world thanks to the internet, which is becoming more and more popular. crime in the e-commerce and online business world is getting worse and bigger.

The obstacles faced by The Police of the Republic of Indonesia in enforcing the law against computer crime and cyber crime

1. Community Legal Awareness

Basically, the job of law enforcement is to keep things fair and in order in the city. Through the criminal justice system and the sentencing system, the rights of people whose rights have been violated by someone's illegal actions will be restored. Cyber crime and computer crime are disgusting acts that break the law and social norms. However, it is hard to find specific laws that control cyber crime and computer crime right now. It is important to know what part the community plays in helping law enforcement fight cyber crime and computer crime so that they can figure out what makes an act of cyber crime or computer crime wrong and unacceptable to the public.

As of now, the Indonesian people still don't seem to know enough about the law when it comes to dealing with online crime and computer crime. This is happening because a lot of people don't understand or know much about the different kinds of online crime and computer crime. Cyber crime and computer crime are hard to stop because people don't have enough knowledge. There are problems with the way the law is set up and with keeping an eye on and controlling the community when there is behaviour that might be connected to cyber crime and computer crime. The first problem is with the process of setting up the law. If people in Indonesia have the right ideas about online crime and computer crime, then society will form a structure, both directly and indirectly.

People may follow this trend because they are afraid of the consequences of criminal threats if they commit cyber crime and computer crime, or because they are aware of it as a legal community. The community's role in monitoring efforts becomes very important when people have a full knowledge of cyber crime and computer crime. This means that when the community doesn't have enough information, the second problem, which is the role of community supervision, won't work (Supriadi, 2020).

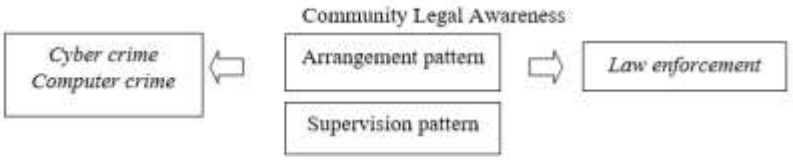

Figure 2 Influence Factors of Public Legal Awareness on Computer Crime and Cyber Crime Law Enforcement

There is a difference between this and common crimes like theft, rape, or murder. Most people know what these common crimes mean, so when someone is accused of committing theft, rape, or murder, the community knows what to expect. The people who live in a community quickly call the police when they see a normal crime happen.

The fact that this pattern of recognising and stopping traditional crimes can be done by anyone shows that criminal behaviour is something that is learned, so it's not impossible that the same thing could be done to stop computer games and other cyber crimes. Based on the differential association theory, this fits with the idea that illegal behaviour is the same as non-criminal behaviour and is learned. So, in order to make people more aware of the law, there needs to be a way to teach people about computer crimes and other common cyber crimes. These are some important ideas that make people more aware of the law:

a. Criminal behavior (in this case cyber crime and computer crime) can be learned and is a learning process.
b. Criminal behavior is learned in interaction with other people through a communication process.
c. An important part of studying criminal behavior occurs in intimate groups.
d. Studying criminal behavior, including techniques for committing crimes and motivation/encouragement or justification for someone committing a criminal act.
e. This particular impulse is learned through understanding the laws and regulations, as well as through the psychological aspect of liking or disliking when committing a crime.
f. A person becomes "delicate" because his appreciation of the laws and regulations prefers breaking them rather than obeying them.
g. This differential association varies depending on frequency, duration, priority and intensity.
h. The process of learning criminal behavior through association with criminal and anti-criminal patterns involves all the mechanisms that apply in every learning process.

Even though criminal behavior is a reflection of general needs and so on, criminal behavior cannot be explained through general needs and values, because non-criminal behavior is also a reflection of general needs and values. the same one.

2. Safety Factor

There's no doubt that the person who commits the crime (cyber crime) will feel safe while doing it. This is because most people use the internet in private places, like their homes, rooms, workplaces, libraries, and even internet shops. People from outside these places have a hard time figuring out what the criminals are doing there. For this reason, it is very uncommon for people outside of the crime scene to know that it is happening. In normal crimes, the person who did the "action" can be easily seen while they are doing it. This is totally different.

Like that, it's hard for other people to see what the criminal is doing when he's out in public. In an internet café without walls, for example, it is hard for regular people to tell when someone is breaking the law. Someone is breaking the law by using a computer for illegal activities, but other people will think he is just using it for fun. This situation will make the bad guy even more daring. Other than that, if someone has done something illegal, they can easily get rid of all evidence of it because the internet has proxy servers that can hide the user's position and delete data or files that have already been sent. So, when the criminal is found, it is hard for police to find proof of the crime.
In this case, too, the part of society and the criminal's own sense of self-worth are both things that affect how safe they feel when they commit a crime. According to criminology, there are two things that can be used to figure out if someone feels safe or not: external factors (like society) and internal factors (like their own self).

Social control and containment theory say this is likely to be the case. This idea says that talking about crime and delinquency is linked to sociological factors like family structure, schooling, and dominant groups. This idea says that people are basically good creatures with good morals (Altheide, 2013). This means that everyone is free to do something. People will have to decide whether to follow the law or break it because they have this freedom.

There are two different kinds of control that can be linked to this theory: personal control and group control. When people say they have "personal control," they mean they can't get what they want by breaking the rules of society. When people talk about "social control," they're talking about how well social groups or institutions in society can enforce rules or norms. The following plan shows how personal and social control play a big part in preventing computer crimes and cyber crimes. This is a common theme that can be taken from the different examples.

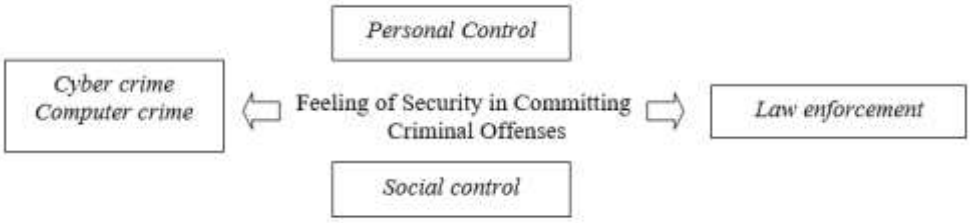

Figure 3 Security Factors in Committing Crimes Against Law Enforcement Computer Crime and Cyber Crime

3. Law Enforcement Factors

Too many police officers are often to blame for the rise in online crime and computer crime. This is because there are still not many police officers who know how to use information technology (like the internet). This means that even after an arrest, police have trouble finding evidence that can be used to catch the criminal. Even more so if the crime has a very complicated way of working. The Indonesian National Police are having trouble getting their staff ready to deal with new types of computer crime and online crime. This problem is becoming more noticeable at the regional level (Galih, 2019). and this is because many police institutions in the regions, like the police station, still don't have internet connections. This is especially true at the police station level.

Being aware of the fact that technology is getting better all the time means that crimes can happen in one place and have effects in other places, even other countries. There are many issues that the Indonesian National Police have to deal with, such as figuring out who has the right to investigate and track down the criminals, finding cyber evidence and figuring out how strong it is, and putting together an official report that doesn't really have an explanation yet. Evidence shows that there is a link between how ready police officers are and As the following graph shows, the rise in computer crime and cyber crime is negatively related to each other.

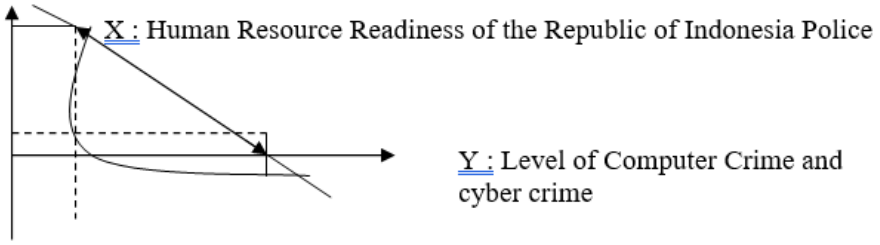

Figure 3 Diagram of the Relationship between Police Readiness of the Republic of Indonesia and Crime Rates

This diagram shows that computer crime and cyber crime go down when the police are more ready and up when they are less ready. This is understandable because the ability of law enforcement officers to deal with the rise of computer crime and the Indonesian Police's

ability to use their human resources and technological resources to find criminal opportunities with the newest IT developments is very important.

4. Factor of Absence of Legal Regulations

Changes in society and the law don't always happen at the same time. This means that changes in the law may happen after changes in other parts of society. In the same way, changes in the law related to computer technology are thought to be very far behind.

It is hard to say that cyber crime and computer crime are crimes in Indonesia because they are subject to the idea of legality. This concept makes it very hard for Indonesian police to enforce the laws that cover cyber crime and computer crime, which are not yet in place. This makes it harder for police to catch people who commit cyber crimes. In addition, the concept of legality doesn't let an analogy be used to decide what is illegal. This kind of situation is known as anomie, which means "normlessness" or "the lack of any norms," or deregulation, which means "the inability of norms to control or regulate behaviour." According to Durkheim's theory of anomie, if a simple society changes into a modern city and society, the inner closeness (intimacy) that is needed to keep a common set of rules will fall apart (Kroedel, 2023). When there isn't a shared set of rules, people in different sectors may act and expect things that are different from those in other sectors. This breaks up groups. Because of this kind of unpredictable behaviour, the system will slowly fall apart, leaving people without any purpose or direction. So, this is what happens when technology moves so quickly ahead of the law and the rule of law falls further behind and loses its power.

Although the Criminal Code normally calls for the death penalty, it is hard for this to apply to computer crimes and online crimes, which are changing quickly and can have effects in many places at once. Because there is no rule that controls their actions, people who commit computer crimes and cyber crimes seem to be in a lawless situation. Being careless about hurting other people in internet creates a domino effect that makes new types of computer crime and cyber crime harder for the police to stop.

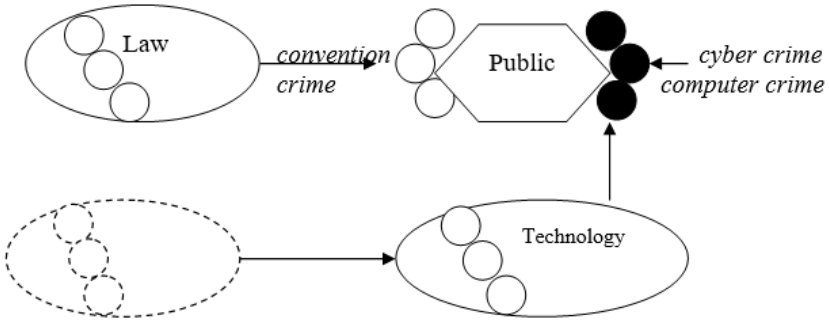

Figure 4 Comparative Image of the Acceleration of Law and Technology

On the other hand, the principle of legality cannot be broken. In real life, however, this principle is not closely followed and exceptions are made. In this day and age of freedom, laws must take into account all aspects of a problem when they are being made. All of the different goals and interests must be brought together so that there is no formal void.

IV. CONCLUSION

Technology is making it easier for people to get information, which is also making it easier for thieves to do bad things in new and changing ways. This is helping computer crime and cyber crime grow quickly. Problems with law enforcement include people not knowing enough about the law, not enough security, police officers not being ready, and not having clear legal rules. In light of the need for developing cyber law right away, it is suggested that the public should be made more aware of the risks of information technology and how to handle cyber

crimes using the most up-to-date methods. There should also be communication platforms set up between law enforcement agencies to help them work together more effectively to fight computer crime and cyber crime. adaptable to the way internet crime works now

REFERENCES

Altheide, D. L. (2013). Media Logic, Social Control, and Fear. *Communication Theory*, *23*(3), 223–238. https://doi.org/10.1111/comt.12017

Antoni, A. (2017). Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online. *Nurani: Jurnal Kajian Syari'ah dan Masyarakat*, *17*(2), 261–274. http://jurnal.radenfatah.ac.id/index.php/Nurani/article/view/1192

Bunga, D. (2019). Legal Response to Cybercrime in Global and National Dimensions. *PADJADJARAN JURNAL ILMU HUKUM (JOURNAL OF LAW)*, *6*(1), Article 1. https://journal.unpad.ac.id/pjih/article/view/19679

Fahmi, T. (2014). KERENTANAN INDONESIA DARI ANCAMAN KEJAHATAN TERORGANISASI (ORGANIZED CRIME) PADA SEKTOR-SEKTOR EKONOMI, KEMANANAN HINGGA POLITIK Oleh. *Jurnal Sosiologi*, *2*(1), 48. https://garuda.kemdikbud.go.id/documents/detail/2230285

Galih, Y. S. (2019). YURISDIKSI HUKUM PIDANA DALAM DUNIA MAYA. *Jurnal Ilmiah Galuh Justisi*, *7*(1), Article 1. https://doi.org/10.25157/jigj.v7i1.2138

Givens, A. (2023). New Knowledge, Better Decisions: Promoting Effective Policymaking Through Cybercrime Analysis. *International Journal of Cybersecurity Intelligence & Cybercrime*, *6*(1). https://doi.org/10.52306/2578-3289.1153

Ishaq. (2017). Metode Penelitian Hukum Dan Penulisan Skripsi, Tesis, Serta Disertasi. Dalam *ALFABETA, cv*.

Kroedel, T. (2023). Norms, epistemic norms, context, and counterfactuals. *Synthese*, *201*(5), 172. https://doi.org/10.1007/s11229-023-04162-x

Mahmud Marzuki, P. (2005). *Penelitian Hukum*. Kencana Prenada Media Group.

Mohammed, K. H., Mohammed, Y. D., & Solanke, A. A. (2019). *Cybercrime and digital forensics: Bridging the gap in legislation, investigation and prosecution of cybercrime in Nigeria*. http://oer.udusok.edu.ng:8080/xmlui/bitstream/handle/123456789/836/Bridging%20the%20gap%20in%20Legislation%20Investigation%20and%20Prosecution%20of%20Cybercrime%20in%20Nigeria.pdf?sequence=1

Mohsin, K. (2021). The Internet and its Opportunities for Cybercrime–Interpersonal Cybercrime. *SSRN Electronic Journal. https://doi. org/10.2139/ssrn*, *3815973*. https://doi. org/10.2139/ssrn 3815973

Oni, S., Araife Berepubo, K., Oni, A. A., & Joshua, S. (2019). E-Government and the Challenge of Cybercrime in Nigeria. *2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG)*, 137–142. https://doi.org/10.1109/ICEDEG.2019.8734329

Puluhulawa, J., Muhtar, M. H., Towadi, M., Swarianata, V., & Apripari. (2023). The Concept of Cyber Insurance as a Loss Guarantee on Data Protection Hacking in Indonesia. *Law, State and Telecommunications Review*, *15*(2), Article 2. https://doi.org/10.26512/lstr.v15i2.44206

Rahman, I., Muhtar, M. H., Mongdong, N. M., Setiawan, R., Setiawan, B., & Siburian, H. K. (2024). Harmonization of Digital laws and Adaptation Strategies in Indonesia focusing on E-Commerce and Digital transactions. *Innovative: Journal Of Social Science Research*, *4*(1), Article 1. https://doi.org/10.31004/innovative.v4i1.8240

Sari, I. (2023). MENGENAL HACKING SEBAGAI SALAH SATU KEJAHATAN DI DUNIA MAYA. *JSI (Jurnal sistem Informasi) Universitas Suryadarma*, *10*(2), Article 2. https://doi.org/10.35968/jsi.v10i2.1086

Shah, I. A., Habeeb, R. A. A., Rajper, S., & Laraib, A. (2022). The Influence of Cybersecurity Attacks on E-Governance. Dalam *Cybersecurity Measures for E-Government Frameworks* (hlm. 77–95). IGI Global. https://doi.org/10.4018/978-1-7998-9624-1.ch005

Siburian, H. K. (2016). Emerging Issue in Cyber Crime: Case Study Cyber Crime in Indonesia. *International Journal of Science and Research*, *5*(11), 511–514.

Supriadi, A. (2020). The Role of the Sub Directorate of Cyber Crime, Ditreskrimsus in Investigating Crime of Cyber Crime. *Law Development Journal*, *2*(3), Article 3. https://doi.org/10.30659/ldj.2.3.412-418

Tanjung, I. U., & Adriani, E. N. (2022). POLITIK HUKUM TERHADAP PENANGGULANGAN KEJAHATAN DUNIA MAYA. *Judge : Jurnal Hukum*, *3*(01), Article 01. https://doi.org/10.54209/judge.v3i01.371

