Journal of Digital Law and Policy
Volume 1 Number 2, January 2022
e-ISSN 2808-3458 p-ISSN 2808-3652
https://ejournal.sidyanusa.org/index.php/jdlp

The Impact of Information Technology Development on Cybercrime Rate in Indonesia

Ni Komang Novia Widiasari[1], Emmy Febriani Thalib[2]

[1,2] *STMIK STIKOM Indonesia, Denpasar, Indonesia*

Email: [1]novia.widiasari@gmail.com , [2]emmy.f@stiki-indonesia.ac.id

Received on	*Revised on*	*Accepted on*
12 January 2022	*24 January 2022*	*28 January 2022*

Abstract

Information technology is growing rapidly in society. In the period of technological development not only gives us a positive impact, but can also have a negative impact. One of the negative impact of the development of information technology is the misuse of the technology, so that it can harm others. Technological developments have an effect on the occurrence of cybercrime in Indonesia, the crimes that have occurred have also developed and varied. The method used in this research are a qualitative approach and descriptive methods. The results of the study show the impact of Information Technology development on the level of cybercrime in Indonesia occurs such as loss of privacy, unauthorized access to important data, data theft and others. Prevention and countermeasures that can be carry out to prevent cybercrime are preventive, pre-emptive and repressive measure

Keywords: Information Technology, Cybercrime.

INTRODUCTION

The development of information technology is currently growing rapidly from time to time, human life today cannot be with the name of information technology. The development of information technology is growing so fast in society that it cannot be denied. People are spoiled by the development of existing information technology. Indonesia, which is a country that has the largest population in the world, is a country that is included in the top five as the world's largest social network user. Information technology entered Indonesia as a form of globalization, which spread so quickly to various parts of the world, information technology has a positive impact on society because it can help and facilitate daily activities, but it is undeniable that existing technology not only has a positive influence, but also gives a negative influence as a result of the misuse of information technology, so that it can harm the community itself. One form of the development of

information technology is the internet. The internet is a system that connects computers to computer networks.[1] Something will be easily obtained with the internet.

Information technology is freely and without limits, people can easily access whatever they want by using the internet and social media that exist as a form of information technology that continues to develop. With the rapid development of available information technology, it is not only used for positive activities but is often used inappropriately for individuals who are not responsible for negative things. The development of information technology that is connected to the internet network from a computer or telephone has been used as a medium for committing crimes. Along with the development of existing information technology has had a negative impact that resulted in the occurrence of cybercrime. Cybercrime is a threat to the public as users of information technology. Cybercrime is a criminal act carried out through the use of available information technology.[2] Cybercrime can also be said as a criminal act carried out through the use of internet information technology which is carried out by attacking public data or personal data that is important or confidentia1.[3] Cybercrimes are committed by entering or using computer facilities or computer networks without obtaining permission through unlawful activities. Cybercrime or cybercrime is like a problem and not an easy thing to overcome.[4] This condition is because cybercrimes committed in cyberspace do not recognize legal boundaries, where when cybercrimes occur then everyone in the virtual world can be involved in the crime, either directly or indirectly, either as perpetrators or victims or just as a witness, this crime can arise without having direct interaction between the perpetrator and the victim. Cybercrimes that often occur in the world are fraud, identity theft, phishing scans and information warfare. Often times this kind of crime is committed one of them to achieve self-satisfaction and economic motives, which is this crime committed in order to gain an advantage for himself or a group to make other individuals lose economically. In Indonesia, cybercrime cases have grown rapidly and become a big concern, in 2013 Indonesia was ranked 2nd in the list of 5 countries with the highest cybercrime rates. The survey reports that the cybercrime index in Indonesia currently reaches 0.62. This value is higher than the global average of 0.54. This means that Indonesia is above average. So, cybercrime is indeed a high risk in Indonesia.[5] The development of existing information technology has resulted in cybercrimes in Indonesia, even cybercrime cases in Indonesia are increasing every year as a result of the impact of information development. In addition, because of the development of information technology, cybercrime cases occur in

---

1 Soni Soni, Afdhil Hafid, and Didik Sudyana, "ANALISIS KESADARAN MAHASISWA UMRI TERKAIT PENGGUNAAN TEKNOLOGI & MEDIA SOSIAL TERHADAP BAHAYA CYBERCRIME," *JURNAL FASILKOM* 9, no. 3 (2019), https://doi.org/10.37859/jf.v9i3.1664.

2 Nurbaiti Ma'rufah, Hayatul Khairul Rahmat, and I Dewa Ketut Kerta Widana, "Degradasi Moral Sebagai Dampak Kejahatan Siber Pada Generasi Millenial Di Indonesia," *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 7, no. 1 (2020).

3 Febrian Kwarto and Madya Angsito, "Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan," *Jurnal Akuntansi Bisnis* 11, no. 2 (2018): 99–110, https://doi.org/10.30813/jab.v11i2.1382.

4 Ni Putu Suci Meinarni and Happy Budyana Sari, "Analisis Potensi Kejahatan Di Dalam Dunia Maya Terkait Data," *Kertha Wicaksana* 14, no. April 2019 (2020): 9–15, https://doi.org/https://doi.org/10.22225/kw.14.1.1530.9-15.

5 Merdeka, "Indonesia Masuk Negara Berisiko Tinggi Terhadap Kejahatan Siber," 2021, 2021, https://www.merdeka.com/uang/indonesia-masuk-negara-berisiko-tinggi-terhadap-kejahatan-siber.html.

Indonesia due to the high level of poverty so that it triggers the level of crime. Cases of cybercrime that often take place in Indonesia vary from embezzlement of bank money, pornography, hacking, carding, spyware and others.[6] Where this case can occur because the perpetrator uses the victim's personal data so that the perpetrator can enter the victim's device. The development of information technology that entered Indonesia led to the occurrence of cybercrimes where the cases that occurred were growing and varied. Even the impact of the Covid-19 virus has an impact on increasing cybercrime cases in Indonesia. Because many people are forced to lose their jobs, so many people commit fraudulent actions under the guise of being someone who asks for benefits or assistance on behalf of the victims of the COVID-19 pandemic.

In Indonesia, the problem of cybercrime has become a concern for both the public and the government, previously there were no ITE Law regulations that specifically regulated cybercrime, before which the cybercrime problem was followed up with laws relating to the problem. But currently cybercrime cases are regulated under the ITE Law. The cybercrime case is regulated in the ITE Law Number 8 of 2011 and subsequently faced with changes to Law No. 19 of 2016, especially in articles 27-30 relating to behaviour that is not recommended to be carried out in cyberspace. Crime in cyberspace cannot be avoided even though a law has been made that regulates it, but every year cybercrime cases in Indonesia are growing. The public is expected to be wiser in responding to existing technological developments, the community is expected to be more careful in providing personal information. Because the development of information technology not only has a positive but also negative influence.

The development of information technology that is increasing should have been of great use to society. With the many developments in existing information technology, we should be able to provide something good for the whole community so that they can easily carry-on life. As in business, work, in addition to studying or education. Therefore, all criminal acts using information technology in carrying out their actions using internet-based systems that can be connected to computers, laptops and other technological devices should have been ended by the use of existing penalties in line with legal certainty based on law and in accordance with the principles of existing justice.

RESEARCH METHODS

This study uses a qualitative approach with a descriptive method, which is an approach in understanding something that exists with a deductive thought process.[7] In qualitative research, it is not in the form of statistics, but through the process of collecting data, which are analysed and then interpreted. In this study, the author will describe the influence of the development of information technology on the level of cybercrime in Indonesia. The object of research is as a target set for the reviewer with the aim and in an effort to obtain something useful and useful in a study. The object of research in this study is the development of information technology on the level of cybercrime in Indonesia, which is the problem that will be discussed in this study.

---

6 Ineu Rahmawati, "Analisis Manajemen Risiko Ancaman Kejahatan Siber," *Jurnal Pertahanan & Bela Negara* Vol.7, no. No.2 (2017).

7 Albi Anggito dan Johan Setiawan, *METODOLOGI PENELITIAN KUALITATIF*, *Jejak* (CV Jejak, 2018).

The source of data used in this study is secondary data, namely data that is not obtained directly by the reviewer, the existing data comes from documents where the data comes from books, articles, scientific works and others related to research problems. Techniques in collecting data as a step used by the reviewer in obtaining data. The technique in collecting data in this study, namely literature study, is a method of collecting data which is carried out through searching for research data and information from written or unwritten documents that support the research process.[8]

FINDINGS

The rapid development of human thinking is influenced by the development of information technology, at this time with the advancement of information technology, people really need information technology, one of which is the internet and will not be able to live without the internet. The internet is a system that is connected to a computer network that can connect without limits from within the country and even throughout the world[9] (With the internet network, one can find out what is happening now and even before in various countries around the world.[10] Information technology is currently growing rapidly. People's lives have gone hand in hand with the development of information technology. Information technology has changed the lives of people who originally lived traditionally without technology, now they have coexisted with modern technology.[11] [12] One of the developments in information technology is the existence of the Internet, the internet has been influential in various aspects of society, one of which is education and business activities, internet users are increasing every year which is also followed by the addition of various internet features, sophisticated cell phones that have been equipped with various facilities that vary from social media such as Instagram, Facebook, WhatsApp and other features. Nowadays people are so facilitated, people can do business activities only by using cell phones, the development of information technology has made it easier for people in various ways.

The positive side of the internet is that it can form a mode of world information technology development with all the behaviour that is carried out. On the other hand, the negative impact of the internet cannot be avoided. The development of internet information technology has resulted in the occurrence of new crimes,

8 Arianto Arianto et al., "Perencanaan Tenaga Pendidik Dan Kependidikan Di Sd Panca Budi Medan," *SABILARRASYAD: Jurnal Pendidikan Dan Ilmu Kependidikan* 4, no. 1 (2019).

9 Machsun Rifauddin and Arfin Nurma Halida, "Waspada Cybercrime Dan Informasi Hoax Pada Media Sosial Facebook," *Khizanah Al-Hikmah : Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan* 6, no. 2 (2018), https://doi.org/10.24252/kah.v6i2a2.

10 Kwarto and Angsito, "Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan."

11 Micah Mahardika, "Kejahatan Siber Hoax Di Ruang Digital Masyarakat Indonesia Melalui Teori Aktivitas Rutin," *Jurnal Kriminologi Indonesia* 16, no. 2 (2020): 11–21.

12 Ni Putu Suci Meinarni and Ida Bagus Ary Indra Iswara, "Hoax and Its Mechanism in Indonesia," *Proceedings of the International Conference of Communication Science Research (ICCSR 2018)*, 2018, https://doi.org/10.2991/iccsr-18.2018.39.

namely cybercrime or crimes committed by utilizing internet channels.[13] The emergence of several cases of cybercrime in Indonesia is a phenomenon that occurs in society, this can happen because of the misuse of existing information technology. The development of information technology has influenced the emergence of crime, this will make it easier for someone to carry out their actions. The development of information technology, especially the internet, has a major influence on the emergence of new crimes with various modes (Perbawa, 2021). One of the crimes that occur as a result of the development of information, especially the internet, is the occurrence of cybercrime. Cybercrime is a crime that violates the law carried out by utilizing the sophistication of the internet by using computer devices. Cybercrime cases that often occur in the community are hacking of a site, data manipulation, wiretapping of other people's data transmissions, credit card theft and others. The phenomenon of cybercrime is one of the criminal acts, both formal and material. It is said to be formal because it involves someone's actions in accessing other people's computer data without the permission of the owner while it is said to be material because the treatment creates material consequences for other individuals such as financial losses. Based on the types of activities carried out by cybercrime cases in Indonesia, they can be grouped including:[14]

1) Unauthorized access is a crime committed by entering a computer software system illegally.
2) Illegal contents, namely crimes committed by entering someone's device and entering data or information that is not true and violates the law on the internet which is intentionally carried out.
3) Data forgery, namely falsifying data on documents owned by an institution or institution.
4) Cyber espionage is a crime carried out by relying on the internet network in carrying out activities on other parties who are targeted by entering the targeted software system.
5) Sabotage is a type of crime that is carried out through the act of disrupting, damaging or destroying a computer program, data or system on a computer network connected to the internet.
6) Cyber stalking, namely the activity of disturbing other individuals through the use of computer networks by using email which is then carried out repeatedly without showing their true identity.
7) Carding is a crime committed in an attempt to steal someone's credit card number and use it for online trading transactions.
8) Hacking is an activity in which someone breaks into someone's data intentionally.
9) Hijacking is a crime that is carried out through piracy of someone's work such as software.

Based on the motives of the activities carried out cybercrime can be classified into two types, namely:[15]

---

13 Ahmad Saudi, "Kejahatan Siber Transnasional Dan Strategi Pertahanan Siber Indonesia," *Fisip* 4 (2017).

14 Mira Herlina and Safarudin Husada, "Dampak Kejahatan Cyber Dan Informasi Hoax Terhadap Kecemasan Remaja Di Media Online," *Promedia* 5, no. 2 (2019).

15 Soni, Afdhil Hafid, and Didik Sudyana, "ANALISIS KESADARAN MAHASISWA UMRI TERKAIT PENGGUNAAN TEKNOLOGI & MEDIA SOSIAL TERHADAP BAHAYA CYBERCRIME."

Cybercrime as a purely criminal act

Pure crime is a criminal act carried out with a criminal motive. These crimes generally use the internet only as a means of crime, for example carding or stealing credit card numbers used to transact online trade.

Compared to conventional crimes, Cybercrime has unique characteristics, namely:[16]

a. Acts carried out illegally, without rights or unethical that occurs in space or cyberspace, making it impossible to determine jurisdiction which country's law applies to action
b. The act is carried out using any (device) that can connect to the internet
c. Loss of material and non-material caused by these actions are often greater than traditional crimes.
d. The perpetrator is a person who can control Internet usage and its applications.
e. The act is often carried out transnational

Cybercrime as a "grey" crime

"Grey" crimes are often difficult to determine if they are criminal acts or not, because this activity is only for gathering information. Based on the target of cybercrime, it can be divided into several categories, namely (Sari, 2018):

1) Cybercrime that attacks a person, a crime carried out with the target of the attack aimed at an individual or someone who has certain characteristics or criteria in line with the target, for example pornography, cyberstalking and cyber-trespass.
2) Cybercrime attacking property rights is a crime carried out to disrupt or attack the rights of other people. For example, accessing computers illegally in an attempt to obtain information.
3) Cybercrime attacks the government, carried out with a specific target, namely to attack the government. Such as cyber terrorism as a treatment that threatens the government.

In today's era with very rapid technological advances and increasing internet users in every point of view of human life. With the increase in internet users, it has a positive and negative impact. The positive impact is that it makes it easier for humans to carry out activities, and the negative impact is the emergence of criminal acts committed by certain parties in carrying out crimes or criminal acts through using the development of information technology through computers with internet facilities.

There are several factors that have the opportunity to have an influence on the occurrence of cybercrime, which are as follows:

a) Political Factor

Observing the many cybercrimes that have occurred in Indonesia with the problems that have been faced by law enforcement officers, the criminalization process in the cyber field has occurred and has harmed many people. The spread of viruses on computers can damage all networks used by governments, banks, all can be

16 Miftakhur Rokhman Habibi and Isnatul Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia," *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam* 23, no. 2 (2020).

affected by chaos in the network system. If the banking computer network system cannot function in a day, it can cause many problems that occur, chaos in payments and financial transactions for customers. With such conditions, it requires a political policy from the Indonesian government to overcome or overcome the development of cybercrime that occurred in Indonesia. Law enforcement officers must put more effort into solving cybercrime crimes that occur. The government has issued Law no. 11 of 2008 concerning ITE to tackle the rise of perpetrators of cybercrime crimes. With legal instruments that have been established, law enforcement officers will enforce the law according to existing laws and enforce them fairly.

b) Economic Factor

Economic development and the advancement of the economy in a country is one of the effects of the promotion of goods produced. An internet and computer networks are media that are no doubt and inexpensive if used as tools and materials to carry out a promotion. People in the world tend to use internet media in carrying out their activities, such as searching for needs and other needs. Indonesia has many handicraft products that are favoured by the international community, such as carvings, statues, and other items. It is hoped that business people can use the benefits of existing information technology, especially with internet facilities. With the development of existing information technology, it is hoped that it will be used wisely and able to promote Indonesia, both in terms of tourism and handicrafts in Indonesia.

c) Socio-Cultural Factors

This socio-cultural factor can be considered through 3 (three) aspects, namely:

1) Advances in Information Technology

The rapid progress of information technology is very unbearable for anyone in Indonesia. Almost every human being needs information technology, not even a few people think that information technology has been used as the most important need, besides food and drink. Not a few people who can one day without the existence of information technology, especially the internet. With the advancement of information technology has a positive and negative impact. The positive impact is that it makes it easier for humans to carry out activities, and the negative impact is the emergence of criminal acts committed by parties who have been determined to carry out crimes or criminal acts through the use of information technology developments through computers with internet facilities.

2) Supervising Human Resources

Information technology has a very close relationship with the supervising operator, the two cannot be separated. Information technology really needs human resources to control the tool itself. So that later we can know whether it is a tool used as a means to achieve public welfare or on the other hand it is used as a tool to damage the interests of other individuals, society, and even more so the interests of the state. Technology has a positive and negative impact, in Indonesia, human resources who manage technology can still be said to be lacking, but human resources who use or use information technology are said to be sufficient. It is hoped that with the supervision of existing human resources, the level of cybercrime in Indonesia can be controlled and reduced.

3) New Community

Technology can be said as a means in an effort to create targets where internet media is used as a communication tool, therefore sociologically it occurs and a new combination is formed in the virtual world where the combination contains people who are addicted to the internet to communicate with each other. , give each other feedback that is thought out based on the principle of balance and freedom between internet addicts in cyberspace. This group as a population of the latest style as a social event, and is very strategic if considered, because through this media there are lessons that we can get. With the existence of communities and internet facilities, many people who initially did not know became aware of something through the community they have, but in every advantage, there must be a drawback, namely with the existence of a new community we must be more vigilant and careful with what is called cybercrime. Due to the rapid development of technology, humans are not aware of carrying out activities in cyberspace and even committing crimes via the internet.[17] The development of information technology today is unavoidable, the community must be ready with various existing technological developments. Apart from the various positive impacts that are given because it can facilitate the community, but also must be prepared for the negative impacts that are given, one of which is cybercrime.[18] The case of cybercrime is a bad influence that occurs due to the growing technology. Cybercrime cases such as the one above requires serious attention with the applicable legal regulations.[19] Cybercrime crimes cannot be controlled quickly, not because they cannot be tackled or prevented, but the shortcomings and limitations that the authorities or our police officers have in uncovering these crimes or cybercrime that make this cybercrime act unable to be tackled and prevented quickly. The number of countries that until now do not have laws and regulation invitation specifically related to the crime. Ways of prevention that can be done to prevent or minimize cybercrime, namely:

1. Protect the cell phone or computer that is used.
2. Avoid using pirated software.
3. Secure personal data used in using social media.
4. Use security devices.
5. Checking and changing passwords
6. Do not carelessly provide personal information.
7. For the government to make laws on cybercrimes.

In strengthening the security of national information systems, a strategic cyber law role is needed[20] for those mentioned above, aside these points are needed:

---

17 Portal Berita Resmi Kepolisian Kepri, "Kajian Soisologis Cyber Crime (Bag 2)," 11 September 2019, 2019.

18 Ma'rufah, Rahmat, and Widana, "Degradasi Moral Sebagai Dampak Kejahatan Siber Pada Generasi Millenial Di Indonesia."

19 Adi Rio Arianto and Gesti Anggraini, "MEMBANGUN PERTAHANAN DAN KEAMANAN SIBER NASIONAL INDONESIA GUNA MENGHADAPI ANCAMAN SIBER GLOBAL MELALUI INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE (ID-SIRTII)," *Jurnal Pertahanan & Bela Negara* 9, no. 1 (2019), https://doi.org/10.33172/jpbh.v9i1.497.

20 Maria M Widiantari, "Proceeding of Conference on Law and Social Studies URGENSI LITERASI ETIKA DIGITAL," *Prosiding Conference On Law and Social Studies*, 2021, 1–15.

1) Securing the System

This is done with the aim of securing the system that we have and preventing any damage to the system that is entered or used by users who we do not want. A security system must have been built and have integrity in all existing subsystems, this has the aim of being able to cover the gap or narrow the land for perpetrators of cybercrime acts to commit crimes. We can do personal security by starting to install the system even to the stage of data security and physical security. Security on system attacks can be done with the network and can be done through implementing Telnet, FTP, Web Server and SMTP security. As for some software that can help strengthen the security of the security system, namely:

a. Internet Firewall

Has a function as an access prevention or gate for unknown parties to enter the internal system. An internet firewall is required on a computer network that is connected to the internet. There are 2 (two) ways to work from the Firewall, namely:

1. Using filters: The function of the firewall filter is to filter communications so that they occur only as needed. Where only computers through a predetermined identity can be connected and certain applications can pass.
2. Using a proxy: This has the function of allowing users to access the internet as widely as possible, but outside it can only access one computer.

b. Cryptography

Cryptography is the art of encoding data. The data to be sent can be filled in with the previous password when the sending process will be carried out from the internet. On the target computer, the data is returned to its original form, so that the recipient can read and understand it. The data is encoded with the aim of so that if there are parties who want to steal the left data, they do not understand the contents of the data because the data sent still resembles a password. In cryptography there are 2 (two) stages that occur, namely:

1. Encryption process: In this process there is a stage of converting the original data into a password data. This step occurs at the time the data is before being sent and this happens on the sender's computer.
2. Decryption process: In this process there is a conversion stage in returning the password data into original data, this step takes place on the recipient's computer. The original data and the data to be encoded are said to be plain text, while the resulting data are said to be cipher text.

c. Secure Sockets Layer (SSL)

The internet is controlled by many people and there are many routes for sending data through the internet. Tapping a data transmission becomes very vulnerable in the era of information technology that is very developed as it is now. Therefore, the browser is equipped or supported through the existence of a secure

socket layer. SSL has a function in encoding data. Where through this stage the computer that is between the computer that sends the data and the one that receives the data cannot re-fill the contents of the data.[21]

2) Law Enforcement

Implementing law reform in law enforcement is the most important thing. Because nowadays, there are many users of information technology who wrongly use the technology by committing crimes, so that cybercrime continues to grow. In today's era, although there has been a law relating to ITE which regulates crimes related to the use of technology, it is very important if a law is made that specializes in cybercrime. Because not all criminal acts in the use of technology can be declared as cybercrime acts, it is hoped that the existing laws are applied fairly and as well as possible. As noted above, the infrastructure and public services that increasingly strategically dependent on information systems, technology, and Indonesian network. The national security paradigm is moving to the side that wider scope, including the protection of citizens. The main task of the state is to provide peace of mind for citizens, including prevention of various cybercrimes. Residents can always feel that their property is under threat. Policy the most important information system security is the legal system national law in the form of cyber law, which regulates cyber actions such as sanctions for malicious and harmful actions. Legal monitoring The Internet has developed relatively recently. Global monitoring being promoted, but enforcement is complicated by the rule of law. This is one of the drawbacks of online law enforcement, especially if concerning crimes committed by individuals or terrorists and business located in another country. The financial sector (FinTech) to have digital financial innovations, including transaction settlement, capital accumulation, investment management, financing and distribution, insurance, market support, other digital financial support, and other service activities.

There is two approaches or theories related to the regulation of law regarding virtual cyber world (cyberspace), namely instrumental theory and theory substantive. Langdon Winner believes that the internet is a common property so that everyone has the full right to be in the cyber world including interacting in it. Therefore, the government does not need making regulations that limit freedom they. Even technology will develop if the government does not control technology and if there are obstacles to the free-market competition is eliminated. But, in reality the people in the virtual world are people from the real world. Society has values and interests, both individually and collectively, which must be protected. Borderless and ubiquitous internet characteristics and transactions which can be done anonymously requires setup. on the other hand, even though it takes place in the virtual world, transactions made by the community have influence in the real world both economically and non-economically economical. A person's rights and obligations can be transferred electronically through the internet.[22]

3) Human Resources Development

---

21 Raodia Raodia, "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)," *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum* 6, no. 2 (2019), https://doi.org/10.24252/jurisprudentie.v6i2.11399.

22 Indriati Amarini, "Pencegahan Dampak Negatif Perkembangan Teknologi Informasi Terhadap Pengguna Internet," *Kosmik Hukum* 18, no. 1 (2018), https://doi.org/10.30595/kosmikhukum.v18i1.2340.

By increasing the knowledge, understanding and expertise possessed by law enforcement officers related to efforts to prevent, investigate and prosecute cases related to cybercrime acts. With the understanding of law enforcement officials regarding cybercrime issues, it can be very helpful, where this will be very useful and able to help someone who is being stricken by cybercrime actions in dealing with and overcoming their cybercrime problems. For example, we also can consider to use a white-collar hacker. They are very intelligent people and have special expertise in the field of technology. This has been exploited or used by the government to overcome cybercrime actions that occurred in Indonesia, hackers can help block networks or sites by irresponsible parties who want to enter the system or attack the system. But this has become a boomerang for law enforcement officials and the government because if it is not carried out as well as possible, hackers may take advantage of the opportunity to steal or damage existing data and networks, therefore implementing this method is important for the government to carry out good supervision.

4) Increase Cooperation between countries

With the rapid development of information technology, cybercrime actions are not only carried out from within the country, but it is possible that the perpetrators of cybercrime acts are in different countries or abroad. For example, the victim of a cybercrime act is in Indonesia or occurs in Indonesia, while the perpetrator of the cybercrime act is abroad. So, from that is the contribution between countries very much need to be implemented in overcoming cybercrime so that it does not spread. This matter in line with developments in the world of international law in preventing cybercrime. One of the recommendations of the United Nations in the VIII congress (Eight Congress on the Prevention of Crime and Treatment of Offenders) which discusses the development of the international information industry as follows.

a. Calling on member countries to intensify preventive efforts in tackling computer abuse by acting as following.
    1) Modernizing formal and material criminal law.
    2) Precautions and computer security.
    3) Increase the sensitivity of citizens and law enforcement officers on the importance of preventing computer crime.
    4) Training or training for law enforcers, especially studying economic crime and computer crime.
    5) Within the framework of education, the ethics of using computers becomes the curriculum field of informatics studies (rules of ethics).
    6) Adopt a computer crime victim protection policy (victim protection) as well as realizing the importance of victims to report.
b. Member countries to actively participate in international forums concerning the prevention of computer crime.
c. Recommend to the Committee on Crime Prevention Control (CCPC) which is a United Nations unit to carry out dissemination to help countries members in the face of computer crime. Consider computer crime cases in terms of implementing the agreement extradition in cybercrime.

CONCLUSION

This paper examines the impact of information technology on our lives so far. We also study the future of our society with more sophisticated developments in the field of information technology and its application in our society. However, there are also negative effects of information technology. We believe the information technology will bring more convenience in life in the future than any negative impact. Information technology development which is all digital brings people into the revolutionary world of business (digital era of revolution) because it is felt to be easier, cheaper, practical and dynamic communicate and obtain information. Yet the prevention and control still needed to avoid the occurrence of various kinds of crimes that take advantage of and are caused by technological development. Countering illegal internet activities is not enough to use criminalization approach. There needs to be cooperation between internet users (users) the government, law enforcement officers, NGOs/NGOs and the community extensively.

REFERENCES

Amarini, Indriati. "Pencegahan Dampak Negatif Perkembangan Teknologi Informasi Terhadap Pengguna Internet." *Kosmik Hukum* 18, no. 1 (2018). https://doi.org/10.30595/kosmikhukum.v18i1.2340.

Arianto, Adi Rio, and Gesti Anggraini. "MEMBANGUN PERTAHANAN DAN KEAMANAN SIBER NASIONAL INDONESIA GUNA MENGHADAPI ANCAMAN SIBER GLOBAL MELALUI INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE (ID-SIRTII)." *Jurnal Pertahanan & Bela Negara* 9, no. 1 (2019). https://doi.org/10.33172/jpbh.v9i1.497.

Arianto, Arianto, Aziza Aziza, Yayi Setia Ningrum, and Candra Wijaya. "Perencanaan Tenaga Pendidik Dan Kependidikan Di Sd Panca Budi Medan." *SABILARRASYAD: Jurnal Pendidikan Dan Ilmu Kependidikan* 4, no. 1 (2019).

Habibi, Miftakhur Rokhman, and Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia." *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam* 23, no. 2 (2020).

Herlina, Mira, and Safarudin Husada. "Dampak Kejahatan Cyber Dan Informasi Hoax Terhadap Kecemasan Remaja Di Media Online." *Promedia* 5, no. 2 (2019).

Kepri, Portal Berita Resmi Kepolisian. "Kajian Soisologis Cyber Crime (Bag 2)." 11 September 2019, 2019.

Kwarto, Febrian, and Madya Angsito. "Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan." *Jurnal Akuntansi Bisnis* 11, no. 2 (2018): 99–110. https://doi.org/10.30813/jab.v11i2.1382.

Ma'rufah, Nurbaiti, Hayatul Khairul Rahmat, and I Dewa Ketut Kerta Widana. "Degradasi Moral Sebagai Dampak Kejahatan Siber Pada Generasi Millenial Di Indonesia." *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 7, no. 1 (2020).

Mahardika, Micah. "Kejahatan Siber Hoax Di Ruang Digital Masyarakat Indonesia Melalui Teori Aktivitas Rutin." *Jurnal Kriminologi Indonesia* 16, no. 2 (2020): 11–21.

Meinarni, Ni Putu Suci, and Ida Bagus Ary Indra Iswara. "Hoax and Its Mechanism in Indonesia." *Proceedings of the International Conference of Communication Science Research (ICCSR 2018)*, 2018. https://doi.org/10.2991/iccsr-18.2018.39.

Merdeka. "Indonesia Masuk Negara Berisiko Tinggi Terhadap Kejahatan Siber." 2021, 2021. https://www.merdeka.com/uang/indonesia-masuk-negara-berisiko-tinggi-terhadap-kejahatan-siber.html.

Rahmawati, Ineu. "Analisis Manajemen Risiko Ancaman Kejahatan Siber." *Jurnal Pertahanan & Bela Negara* Vol.7, no. No.2 (2017).

Raodia, Raodia. "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)." *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum* 6, no. 2 (2019). https://doi.org/10.24252/jurisprudentie.v6i2.11399.

Rifauddin, Machsun, and Arfin Nurma Halida. "Waspada Cybercrime Dan Informasi Hoax Pada Media Sosial Facebook." *Khizanah Al-Hikmah : Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan* 6, no. 2 (2018). https://doi.org/10.24252/kah.v6i2a2.

Saudi, Ahmad. "Kejahatan Siber Transnasional Dan Strategi Pertahanan Siber Indonesia." *Fisip* 4 (2017).

Setiawan, Albi Anggito dan Johan. *METODOLOGI PENELITIAN KUALITATIF*. *Jejak*. CV Jejak, 2018.

Soni, Soni, Afdhil Hafid, and Didik Sudyana. "ANALISIS KESADARAN MAHASISWA UMRI TERKAIT PENGGUNAAN TEKNOLOGI & MEDIA SOSIAL TERHADAP BAHAYA CYBERCRIME." *JURNAL FASILKOM* 9, no. 3 (2019). https://doi.org/10.37859/jf.v9i3.1664.

Suci Meinarni, Ni Putu, and Happy Budyana Sari. "Analisis Potensi Kejahatan Di Dalam Dunia Maya Terkait Data." *Kertha Wicaksana* 14, no. April 2019 (2020): 9–15. https://doi.org/https://doi.org/10.22225/kw.14.1.1530.9-15.

Widiantari, Maria M. "Proceeding of Conference on Law and Social Studies URGENSI LITERASI ETIKA DIGITAL." *Prosiding Conference On Law and Social Studies*, 2021, 1–15.