The Implementation of The Cybercrime Prevention Policy at The Metro Jaya Police Station in Central Jakarta

1st Dian Damayanti[1], 2nd Mary Ismowati[2]
{diandamayanti17@gmail.com[1], mary.ismowati@stiami.ac.id[2]}

Magister of Administrative Science Study, Institut Ilmu Sosial dan Manajemen STIAMI[1,2]

Abstract. The research aims to determine the implementation of policies regarding cybercrime applications at the Metro Jaya Police, Central Jakarta in accordance with the Electronic Transactions of Electronic Information and / or Electronic Documents regulations. The basic theory used in this research is Edward III (1980), which states that policy implementation is influenced by communication, resources, disposition, and bureaucratic structures. This study used a qualitative descriptive method by interviewing several informants. The results showed that the Central Jakarta Metro Jaya Police had implemented a cybercrime prevention policy through communication, resources, disposition, and bureaucratic structures to overcome cybercrime. Barriers to policy implementation are limited personnel such as IT and cyber forensics experts, budget and facilities and infrastructure to support the disclosure of cybercrime cases. Training is needed for cyber police in using technology, both by the police and universities. This step is necessary to recruit information technology experts. The urgency of the need for experts must also be balanced with the presence of sophisticated facilities and infrastructure to support network security and also to facilitate tracking criminals so that cybercrime cases can be resolved quickly.

Keywords: Policy Implementation, Cyber Crime, Prevention, Impact, and Law on Information and Electronic transaction.

1 Introduction

Indonesia Ranks 70 for Cyber Crime Cyber defense in Indonesia is influenced by two main factors, namely infrastructure and reliable technology and awareness that cyber-world security is an important issue. This was conveyed in the Board of Conferences #12 of the National Conference 2017 at JIEXPO Commercial Center, Monday (10/23/2017). Speaker Faizal Djoemadi representative of Telekomunikasi Indonesia Internasional said that Indonesia still needs to upgrade its infrastructure and technology.

"But the physical and logic [software] layers can be purchased. The most urgent one indeed is cultural factor or awareness that security in cyber world is essential," said Faizal, in Jakarta, Tuesday (10/24). Until now, according to Faizal, Indonesia still places in position 70 of 193 countries in terms of cybercrime strategy. This certainly still becomes homework in an effort to implement the cyber defense of Indonesia.

Awareness and literacy for cyber activity on cyber networks is needed by internet users. The Special Capital Region of Jakarta (DKI Jakarta) is the capital city and the largest city in

ICSTIAMI 2019, July 17-18, Jakarta, Indonesia
Copyright © 2021 EAI
DOI 10.4108/eai.17-7-2019.2302054

Indonesia. Jakarta is the only city in Indonesia that has provincial level status. Jakarta is located on the northwest coast of Java. Formerly known by several names including Sunda Kelapa, Jayakarta, and Batavia. In the international world, Jakarta also has the nickname J-Town, or more popularly The Big Durian because it is considered a comparable city of New York City (Big Apple) in Indonesia.

The Jakarta metropolitan area (Jabodetabek), which has a population of around 28 million, is the largest metropolitan in Southeast Asia or second in the world. As a center of business, politics and culture, Jakarta is home to the headquarters of state-owned companies, private companies, and foreign companies.

The *Metro Jaya Police station in Jakarta Central* will apply the law on cybercrime. A legal entity should work with IT experts to tackle such crimes. To reveal who will be responsible for the crime, an IT expert should be able to perform network forensics to find out the origin and source of the offense. This strategy is expected to reduce or eradicate crimes committed in the world of technology.

Implication of cybercrime policy at the Metro Jaya Police Station in Central Jakarta has a strong legal basis, namely Law Number 19 of 2016 article 1, regarding electronic transactions of Electronic Information and / or Electronic Documents and / or printed results that are legal legal evidence Electronic Information is one or a collection of electronic data, including but not limited to writing, sound, images, maps, designs, photos, electronic data interchange (EDI), electronic mail (electronic mail), telegram, telex, telecopy or the like, letters, signs, numbers, Access Codes, symbols, or processed perforations that have meaning or can be understood by people who are able to understand them.

Research Question : How is the implementation of the cybercrime prevention policy at the Metro Jaya Police Station in Central Jakarta? What obstacles have been faced in implementing the policy of implementing cybercrime prevention at the Metro Jaya Police Station in Central Jakarta? What are the efforts made in implementing the cybercrime prevention policy at the Metro Jaya Police Station in Central Jakarta?

2 Implementation Policy

Attitude that will bring on themselves offender disposition policies. High disposition by Edward III (1980) and Van Horn and Van Meter (1975) effect on the rate of successful implementation of the policy. Disposition for Edward III (1980:53) is defined as the tendency, desire or agreement of the executive to implement the policy. If you want to be successful policy implementation effectively and efficiently, the executor is not just knowing what to do and have the willingness to carry out that policy, but they also have to have the will to implement the policy. The role of the actors in policy implementation is proposed by Edwards III (1980: 12) who states that "Public policies are made and implemented on the national, state, and local levels. Often implemented by lower level by units of government. " This suggests that public policy is made and implemented at the national level, state, and local government. Edward III (1980: 12) holds that policy implementation is influenced by four variables, namely:

1. Communication, namely the success of policy implementation requires that the implementor know what must be done, where the policy goals and objectives must be transmitted to the target group, thereby reducing the distortion of implementation.

2. Resources, even though the contents of the policy have been communicated clearly and consistently, but if the implementor lacks the resources to implement, the implementation will not be effective. These resources can be tangible human resources, for example the competence of the implementor and financial resources.
3. Disposition, is the character and characteristics possessed by the implementor, such as commitment, honesty, democratic nature. If the implementor has a good disposition, then the implementor can run the policy well as what is desired by policy makers. When the implementor has a different attitude or perspective than the policy maker, the policy implementation process also becomes ineffective.
4. Bureaucratic Structure, Organizational structure tasked with implementing policies has a significant influence on policy implementation. The aspect of organizational structure is Standard Operating Procedure (SOP) and fragmentation. Organizational structures that are too long will tend to weaken supervision and lead to red-tape, which is a complex and complex bureaucratic procedure, which makes organizational activities inflexible.

However, policy implementation has several inhibiting factors. The organizational structure of implementation may cause problems if the division of powers and responsibilities is less tailored to the division of tasks or marked by the limitation of the less obvious limitations (DeLeon P and L DeLeon 2002)

As for the obstacles in the implementation of the policy, a solution to overcome needs to meet soon. A policy will be effective if during the making and the implementation is supported by adequate facilities.

Cyber Crime

According to (Peter Stephenson, 2000) Cybercrime is “The easy definition of cybercrime is crimes directed at a computer or a computer system. The nature of cybercrime, however, is far more complex. As we will see later, cybercrime can take the form of simple snooping into a computer system for which we have no authorization. It can be the feeing of a computer virus into the wild. It may be malicious vandalism by a disgruntled employee. Or it may be theft of data, money, or sensitive information using a computer system. In two The UN Congress document cited by (Barda Nawawi Arief, 2007) concerning the Prevention of Crime and Treatment of Offenders in Havana Cuba in 1990 and in Vienna Austria in 2000, explained the existence of two terms related to the definition of Cybercrime, namely cybercrimes and computer related crime.

Cybercrime is a term that refers to criminal activity with a computer or computer network into a tool, target or scene of the crime. Included therein to include an online auction fraud, check forgery, credit card fraud (carding), confidence fraud, identity fraud, child pornography, etc. In the Internet, security issues are indispensable.

For without security, data on existing systems on the Internet can be stolen by irresponsible people. Often an Internet-based network system has flaws or often called a security hole. If the hole is not closed, a thief can enter from the hole. Theft of data and systems from the Internet, including in the case of computer crime. Cybercrime is a crime that is often done on the Internet.

Cyber Crime Types

Based on the type of activities done, cybercrime can be classified into several types as follows:

1. Unauthorized Access

2. Illegal Contents
3. Intentional spread of virus
4. Data Forgery
5. Cyber Espionage, Sabotage, and Extortion
6. Cyberstalking
7. Carding
8. Hacking and Cracking
9. Cybersquatting and typosquatting
10. Hijacking.
11. Cyber Terrorism

Crime Prevention

"Prevention is the first imperative of justice " (United Nations document S/2004/616, para. 4)*"Crime Prevention comprises strategies and measures that seek to reduce the risk of crimes occurring, and their potential harmful effects on individuals and society, including fear of crime, by intervening to influence their multiple causes." Guidelines for the Prevention of Crime ECOSOC Resolution 2002/13, Annex.*

Crime prevention is a multi-sectoral, multi-disciplinary, and integrated endeavour.

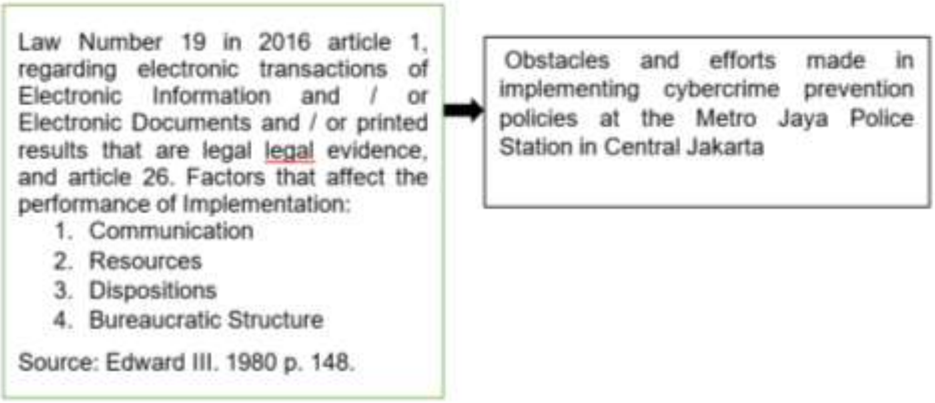
The introduction to the Guidelines for the Prevention of Crime indicates that: *"There is clear evidence that well-planned crime prevention strategies not only prevent crime and victimization, but also promote community safety and contribute to sustainable development of countries. Effective, responsible crime prevention enhances the quality of life of all citizens. It has long-term benefits in terms of reducing the costs associated with the formal criminal justice system, as well as other social costs that result from crime." (Economic and Social Council resolution 2002/13, annex),* (above) .

Recognizing the multiple causes of crime and as the custodian of the United Nations standards and norms in crime prevention and criminal justice, UNODC promotes strategies, plans, and programmes, which are multi-sectoral, multi-disciplinary, and which favour civil society participation. Such strategies and action plans are underpinned by the **basic principles for the prevention of crime** *(Guidelines for the Prevention of Crime, ECOSOC Resolution 2002/13, Annex)* (above):

1. **Government leadership** at all levels is required to create and maintain an institutional framework for effective crime prevention.
2. **Socio-economic development and inclusion** refer to the need to integrate crime prevention into relevant social and economic policies, and to focus on the social integration of at-risk communities, children, families, and youth.
3. **Cooperation and partnerships** between government ministries and authorities, civil society organizations, the business sector, and private citizens are required given the wide-ranging nature of the causes of crime and the skills and responsibilities required to address them.
4. **Sustainability and accountability** can only be achieved if adequate resources to establish and sustain programmes and evaluation are made available, and clear accountability for funding, implementation, evaluation and achievement of planned results is established.

5. **Knowledge base** strategies, policies and programmes need to be based on a broad multidisciplinary foundation of knowledge, together with evidence regarding specific crime problems, their causes, and proven practices.
6. **Human rights/rule of law/culture of lawfulness** the rule of law and those human rights which are recognized in international instruments to which Member States are parties must be respected in all aspects of crime prevention, and a culture of lawfulness actively promoted.
7. **Interdependency** refers to the need for national crime prevention diagnoses and strategies to take into account, where appropriate, the links between local criminal problems and international organized crime.
8. The principle of **differentiation** calls for crime prevention strategies to pay due regard to the different needs of men and women and consider the special needs of vulnerable members of society (https://www.unodc.org/unodc/en/justice-and-prison-reform/CrimePrevention.html)

The model implementation of the cybercrime prevention policy at the Metro Jaya Police Station in Central Jakarta



Law Number 19 in 2016 article 1, regarding electronic transactions of Electronic Information and / or Electronic Documents and / or printed results that are legal legal evidence, and article 26. Factors that affect the performance of Implementation:

1. Communication
2. Resources
3. Dispositions
4. Bureaucratic Structure

Source: Edward III. 1980 p. 148.

Obstacles and efforts made in implementing cybercrime prevention policies at the Metro Jaya Police Station in Central Jakarta

3 Methodology

This research used Qualitative approach for exploring and understanding the meaning individuals or groups ascribe to a social or human problem. The process of research involves emerging questions and procedures. Data typically collected in the participant's setting. data analysis inductively building from particulars to general themes. and the researcher making interpretations of the meaning of the data. The final written report has a flexible structure.

The first data coding system that was piloted involved "open coding": an emergent coding technique drawn from grounded theory methodology (Glaser& Strauss, 1967; Strauss& Corbin, 1998).

Informants consit of : Head of Section of the Special Criminal Regiment Unit of the Metro Jaya Central Jakarta Regional Office, People who work as entrepreneurs. who lives in the Central Jakarta area, Head of the special criminal unit of the Metro Jaya Regional Police of DKI Jakarta Office**,** Head of Civil Service Section of Metro Jaya Regional Office, Central Jakarta,Position of the chief the finance department of the Metro Jaya Regional Office in Central Jakarta, Head of the licensing section of the Metro Jaya Regional Office in Central Jakarta and Head of the Community Guidance Section of the Central Jakarta Metro Jaya Regional Office.

4 Discussion

1. The implementation of the cybercrime prevention policy at the Metro Jaya Police Station in Central Jakarta.

The implementation of the cybercrime prevention policy at the Metro Jaya Police Station in Central Jakarta the success of policy implementation requires that the implementor know what must be done, where the policy goals and objectives must be transmitted to the target group, thereby reducing the distortion of implementation. The application of the prevention of cyber transactions at the Jakarta Police Station has a strong legal basis, namely Law Number 19 of 2016 concerning electronic transactions 1, regarding electronic information and / or electronic documents that are legal legal evidence , and article 26. cross and use the concept of Edward III (1980) (in Subarsono, 2011: 90-92). The following is the explanation of the analysis of the implementation of the Jakarta police station's cybercrime in the central prevention policy based on the conceptual framework of adoption researchers using the theory of Edward III (1980), holds that policy implementation is influenced by four variables, namely: Communication, resources, disposition, and bureaucratic structure. Based on the answers of the informants in table 4.1 above, it is known that the answers to the implementation of cybercrime prevention policies at the Central Jakarta Police Station can be explained as follows:

The results of the open coding state of the implementation of cybercrime prevention policies in the central Jakarta polres, namely: Cyberspace cyber partoli, cooperation, prevention, collaborate with the Office of the Cyber Cyber Crime Investigations Satellite Office involving children in cyberspace. (Inf 1, Inf 2, Inf 3, Inf 4, Inf 5, Inf 6, Inf 7).

Based on this, axial coding regarding the state of implementation of prevention policies for cybercrime in central Jakarta polres, namely: online partoli, government cooperation and communication service providers companies. Victims of cybercrime: Children. Formation of the unit: Police Office for Crime Metro Investigation of Cyber Crime Establishment of bodies: Satellite Office for Cyber Crime Investigation.

From open coding and axial coding, conclusions can be made on selective coding that the implementation of cybercrime prevention policies in central Jakarta polres, namely: online partoli, government cooperation and communication service providers companies. Victims of cybercrime: Children. Formation of the unit: Police Office for Crime Metro Investigation of Cyber Crime Establishment of bodies: Satellite Office for Cyber Crime Investigation. in accordance with law no 19 of 2016 concerning electronic transactions 1, regarding electronic information and / or electronic documents that are legal legal evidence , and article 26. cross and use the concept of Edward III (1980) (in Subarsono, 2011: 90-92).

a. Communication.

The implementation of the cybercrime prevention policy at the Metro Jaya Police Station in Central Jakarta the success of policy implementation requires that the implementor know what must be done, where the policy goals and objectives must be transmitted to the target group, thereby reducing the distortion of implementation.

Based on the answers of the informants, it is known that the answers to communication in the implementation of cybercrime prevention policies can be explained as follows. the Cybercrime prevention policy? explain the obstacles and innovations used in countering cybercrime! The results of the open coding state of communication implementing the prevention of cybercrime policies are from (INF 1, INF 2, INF 3, INF 4, INF 5, INF 6, INF 7) posted on the bulletin board.

From open coding and axial coding, conclusions can be made on selective coding that communication in the implementation of cybercrime prevention policies namely Communication, Socialized about Maya World Crime prevention policies, barriers and innovations: Brochures posted on the bulletin board. Barriers to resources are: limited budget funds. In adequate facilities and infrastructure. Human resources, namely: limited personnel, lack of IT experts and cyber forensics Procedural barriers: Information technology laws. Innovations on resources are: adequate facilities and infrastructure. Human resource efforts, namely: personnel training, cooperation, empowering IT experts and universities. Formation of the unit: Police Office for Crime Metro Investigation of Cyber Crime Establishment of bodies: Satellite Office for Cyber Crime Investigation.

Based on the answers of the informants above it is known that the answers to communication Mention the results of the evaluation of the Cybercrime prevention policy in the Metro Jaya Police Chief, Central Jakarta! The results of the open coding state of communication implementing the prevention of cybercrime policies are from (INF 1, INF 2, INF 3, INF 4, INF 5, INF 6, INF 7) Cybercrime prevention policy evaluation of Cybercrime prevention policies: lack of socialization of lack of knowledge of cybercrime prevention, lack of supervision.

Based on this, axial coding regarding communication in the implementation of cybercrime prevention policies namely Evaluation results, prevention of cybercrime: Cybercrime prevention policy evaluation of Cybercrime prevention policies: lack of socialization of lack of knowledge of cybercrime prevention, lack of supervision. from the open coding and axial coding above can be made a conclusion selective coding that communication in the implementation of cybercrime prevention policies in central Jakarta polres, namely Cybercrime prevention policy evaluation of Cybercrime prevention policies: lack of socialization of lack of knowledge of cybercrime prevention, lack of supervision.

b. Resources.

Barriers to resources are: limited budget funds. inadequate facilities and infrastructure. Human resources, namely: limited personnel, lack of IT experts and cyber forensics Procedural barriers: Information technology laws. Innovations on resources are: adequate facilities and infrastructure. Human resource efforts, namely: personnel training, cooperation, empowering IT experts and universities. Formation of the unit: Police Office for Crime Metro Investigation of Cyber Crime Establishment of bodies: Satellite Office for Cyber Crime Investigation. Based on this, axial coding regarding communication of cybercrime prevention communication policies, socialized about Maya World Crime prevention policies, barriers and innovations: Brochures posted on the bulletin board. Barriers to resources are: limited budget funds. inadequate facilities and infrastructure.

Human resources, namely: limited personnel, lack of IT experts and cyber forensics Procedural barriers: Information technology laws. Innovations on resources are: adequate facilities and infrastructure. Human resource efforts, namely: personnel training, cooperation, empowering IT experts and universities. Formation of the unit: Police Office for Crime Metro Investigation of Cyber Crime Establishment of bodies: Satellite Office for Cyber Crime Investigation.

Based on the answers of the informants, it is known that the answers regarding resources in the implementation of the Resource World cybercrime prevention policy. Is there an increase in quality and quantity and continuous improvement of employee performance and socialization of excellent service culture? explain what obstacles are in resources? The results of the open coding state of the resource implementation of cyberrime prevention policies according to (INF 1, INF 2, INF 3, INF 4, INF 5, INF 6, INF 7) are Human Resources improve quality and quantity by: training and scholarship.

Based on this, the above axial coding is about the resource for implementing cybercrime prevention policies, namely Resource: quality, quantity, performance, obstacles and socialization of excellent service culture. Human resources improve quality and quantity by: training and scholarship. Socialization of excellent service culture, namely: Information desk staff & complaints must provide excellent service. Reliable communication skills are also important in understanding what the public wants, focusing on the community, providing efficient services, a personal approach, and good relations with the community. Show sympathy, talk with feelings, and give solutions to show that you understand the desires of the community. Ask for feedback from the community in the form of a service satisfaction survey to improve if there are deficiencies in services.

Barriers to resources are: limited budget funds. inadequate facilities and infrastructure. Human resources, namely: limited personnel, lack of IT experts and cyber forensics Procedural barriers: Information technology laws. Efforts on resources are: adequate facilities and infrastructure.Human resource efforts, namely: personnel training, cooperation, empowering IT experts and universities. Formation of the unit: Police Office for Crime Metro Investigation of Cyber Crime Establishment of bodies: Satellite Office for Cyber Crime Investigation. From open coding and axial coding, a conclusion can be made on selective coding that is a resource in the implementation of cybercrime prevention policies, namely quality, quantity, performance, obstacles and socialization of excellent service culture. Human resources improve quality and quantity by: training and scholarship.

Socialization of excellent service culture, namely: Information desk staff & complaints must provide excellent service. Reliable communication skills are also important in understanding what the public wants, focusing on the community, providing efficient services, a personal approach, and good relations with the community. Show sympathy, talk with feelings, and give solutions to show that you understand the desires of the community. Ask for feedback from the community in the form of a service satisfaction survey to improve if there are deficiencies in services. Barriers to resources are: limited budget funds. Inadequate facilities and infrastructure. Human resources, namely: limited personnel, lack of IT experts and cyber forensics Procedural barriers: Information technology laws. Efforts on resources are: adequate facilities and infrastructure.

Human resource efforts, namely: personnel training, cooperation, empowering IT experts and universities. Formation of the unit: Police Office for Crime Metro Investigation of Cyber Crime Establishment of bodies: Satellite Office for Cyber Crime Investigation. Based on the answers of the informants in table 4.5 above, it is known that the answers regarding resources in the implementation of the Resource World cybercrime prevention policy. Are the facilities and infrastructures in the Central Jakarta Metro region in overcoming cybercrime sufficient?

The results of the open coding state of the resource implementation of cyberrime prevention policies according to (INF 1, INF 2, INF 3, INF 4, INF 5, INF 6, INF 7) new buildings, equipment, and updated.. Based on this, the above axial coding is about the resource for implementing cybercrime prevention policies, namely Facilities and infrastructures cybercrime: new buildings, equipment, and updated.

From open coding and axial coding, a conclusion can be made on selective coding that is a resource in the implementation of cybercrime prevention policies, namely Facilities and infrastructures cybercrime: new buildings, equipment, and updated.

c. Disposition

Based on the answers of the informants, it is known that the answers regarding Attitude / disposition in the implementation of cybercrime prevention policies.

The results of open coding attitude / disposition in implementing cybercrime prevention policies namely awards: promotion of promotions, and salary increases. punishment: reprimand, sacking of dismissal. from (INF 1, INF 2, INF 3, INF 4, INF 5, INF 6, INF 7). Based on this, the axial coding regarding Attitude / disposition in implementing cybercrime prevention policies namely awards: promotion of promotions, and salary increases. punishment: reprimand, sacking of dismissal. From the open coding and axial coding, we can make a conclusion of selective coding that attitudes / dispositions in implementing cybercrime prevention policies namely awards: promotion of promotions, and salary increases. punishment: reprimand, sacking of dismissal.

Based on the answers of the informants, the obstacles in disposition. Can be explained as follows : limited personnel, lack of IT experts and cyber forensics Procedural barriers: Information technology laws. Efforts on resources are: adequate facilities and infrastructure.

d. Bureaucratic structure.

Based on the answers of the informants, it is known that the answers to the structure of bureaucracy in the implementation of cybercrime prevention policies in the Central Jakarta Regional Office, Central Jakarta have an ideal for cybercrime services, conduct reviews and have units that manage cybercrime services, and evaluate the implementation of cybercrime? can be explained as follows.

The results of open coding regarding bureaucratic structure in the implementation of cybercrime prevention policies are standard operational procedures for cybercrime. policy evaluation: lack of socialization of cybercrime, not knowing about cybercrime, easy access to information without being processed by news hoaxes. Based on this, axial coding regarding the structure of bureaucracy in implementing policies to prevent cybercrime, namely Bureaucratic structures, Standard operational procedures, cybercrime services, units, manage, evaluation. standard operational procedure for cybercrime. policy evaluation: lack of socialization of cybercrime, not knowing about cybercrime, easy access to information without being processed by news hoaxes. From the open coding and axial coding above, we can draw conclusions about selective coding that is Bureaucratic structure, Standard operational procedures, cybercrime services, units, manage, evaluation. standard operational procedure for cyber crime. policy evaluation: lack of socialization of cybercrime, not knowing about cybercrime, easy access to information without being processed by news hoaxes.

2. Obstacles have been faced in implementing the policy of implementing cybercrime prevention at the Metro Jaya Police Station in Central Jakarta

Obstacles have been faced in implementing the policy of implementing cybercrime prevention at the Metro Jaya Police Station in Central Jakarta The number of "players" (actors) involved: the more parties involved and also influence the implementation, the more complicated the communication the more likely there are obstacles in the implementation process.

There is double commitment or loyalty: In many cases, the parties involved or someone who should have a role in success in determining or approving a project in the implementation are still experiencing delays due to commitment to the project, time taken by other tasks or another program. The inherent complexity of the project itself: In this case in the form of technical factors, economic factors, procurement of materials and implementing behavioral factors and the community

Too many levels of decision making: More levels and places of decision making that are needed before the project plan is implemented. Likewise, at the operation stage, the distribution of funds and donations needed is time consuming because it requires the approval of many parties.

Time factor and leadership change: The longer the time required from when planning with implementation, the more likely the implementation faces obstacles especially if there is a policy change. according to the results of the interview with the resource person.

The results of the open coding state of obstacles have been faced in implementing the policy of implementing cybercrime prevention at the Metro Jaya Police Station in Central Jakarta namely: Barriers to resources are: limited budget funds. inadequate facilities and infrastructure. Human resources, namely: limited personnel, lack of IT experts and cyber forensics. Procedural barriers: Information technology law. (Inf 1, Inf 2, Inf 3, Inf 4, Inf 5, Inf 6, Inf 7).

Based on this, the axial encoding of barriers to implementation of cyber crime prevention policies at the Central Jakarta Police Station, namely: Barriers to resources are: limited budget funds. inadequate facilities and infrastructure. Human resources, namely: limited personnel, lack of IT experts and cyber forensics. Procedural barriers: Information technology laws.

From open coding and axial coding, conclusions can be drawn about selective coding that the implementation of cyber crime prevention policies in the Central Jakarta police station, namely: Barriers to resources are: limited budget funds. inadequate facilities and infrastructure. Human resources, namely: limited personnel, lack of IT experts and cyber forensics. Procedural barriers: Information technology laws. In accordance with law no 19 of 2016 concerning electronic transactions 1, regarding electronic information and / or electronic documents that are legal legal evidence.

3. The efforts made in implementing the cybercrime prevention policy at the Metro Jaya Police Station in Central Jakarta.

Driving Factors (Facilitating Conditions: Commitment of political leaders: in practice it is primarily a commitment from government leadership because government leadership is essentially covered by political leaders in power in the region. Organizational ability: in the implementation phase of the program the essence can be interpreted as the ability to carry out tasks, as determined or charged to an organizational unit.

Based on the answers of the informants, it is known about the answers to assistance in relation to requests for cybercrime at the Jakarta Police Station. The results of open coding have been faced in an effort to implement the policy of implementing cybercrime prevention at the Metro Jaya Police Office in Central Jakarta, namely: Efforts on resources are: adequate facilities and infrastructure.

Human resource efforts, namely: personnel training, cooperation, empowering IT experts and universities.

Formation of the unit: Police Office for Crime Metro Investigation of Cyber Crime Establishment of bodies: Satellite Office for Cyber Crime Investigation. (Inf 1, Inf 2, Inf 3, Inf 4, Inf 5, Inf 6, Inf 7).

Based on this, the axial encoding of has been faced in an effort to implement a policy of implementing cybercrime prevention at the Metro Jaya Police Station in Central Jakarta, namely: Effort, prevention, cybercrime: Efforts on resources are: adequate facilities and infrastructure. Human resource efforts, namely: personnel training, cooperation, empowering IT experts and universities. Formation of the unit: Police Office for Crime Metro Investigation of Cyber Crime Establishment of bodies: Satellite Office for Cyber Crime Investigation.

From open coding and axial coding, conclusions can be drawn about selective coding that have been faced with efforts to implement the policy of implementing cybercrime prevention at the Metro Jaya Police Station in Central Jakarta, namely: Effort, prevention, cybercrime: Efforts on resources are: adequate facilities and infrastructure. Human resource efforts, namely: personnel training, cooperation, empowering IT experts and universities. Formation of the unit: Police Office for Crime Metro Investigation of Cyber Crime Establishment of bodies: Satellite Office for Cyber Crime Investigation.

5 Conclusion

Based on the results of the research on the implementation of the policies to combat cybercrime in the Metro Jaya Regional Office Central Jakarta in accordance with law no 19 of 2016 concerning electronic transactions.

1. That policy implementation is influenced by four variables, namely: Communication, resources, disposition, and bureaucratic structure. And the results of the research and discussion on the analysis of the implementation of the policies to overcome cybercrime in the Central Jakarta Regional Office of Jakarta.
2. The obstacle Limited constraints of personnel such as IT and cyber forensic experts, another crucial obstacle is the limited operational budget funds, a crucial problem besides legal instruments, namely insufficient human resources, budget and facilities and infrastructure to support disclosure of cybercrime cases. From the information obtained by the authors of the police department, they are still not too literate about technology, even many members of the cyber police Indonesia are still using computers. It could be said that Indonesian polyclinic ability in cyberspace is still in the standard stage or beginner.
3. There are trainings either by the police or the state or private universities and colleges in the information technology faculty. This step needs to be done to recruit information

technology experts, especially students and students who have expertise in the field of IT (Information technology). The urgency of the needs of experts must also be balanced with the presence of advanced facilities and infrastructure and equipment facilities to support network security and also to facilitate tracking of perpetrators of crimes so that cases of cybercrime can be quickly resolved. The existence of cyber patrols to reduce the number of crimes involving children in cyberspace, we will collaborate with related parties such as the telkom and the Minister of Communication and Information. Cyber patrols are carried out to prevent cybercrime involving minors and the operation of the cybercrime investigation headquarters, the Metro Crime Police Office Cyber Crime Investigations Satellite Office

Suggestion

In the implementation of the implementation of the cybercrime prevention policy in the Metro Jaya Regional Office Central Jakarta, namely:

1. The improvement of the cybercrime service delivery system must have experts who must be provided in the Jakarta Metro Jaya Regional Office and good coordination with the Ministry of Communication and Information.
2. Improvements from the private sector are in the form of providing service providers such as Telkomsel, and others. To improve the service system again and impact Implementation of the cybercrime prevention policy at the Metro Jaya Police Station in Central Jakarta: Increase parental awareness and attention to child supervision. The National Police of the Republic of Indonesia has also launched a child protection program on the internet (save children on the internet). State Code and Cyber Codes (BSSN). Sociocultural approaches and community socialization through seminars, training and competitions.
3. Whereas the efforts made in the implementation of the policies to combat cybercrime in the Central Jakarta Regional Office of Jakarta, namely improvements in all aspects, namely when coordinating the division of tasks in implementing cybercrime prevention policies, there must be improvements in human resources, facilities and infrastructure.

References

[1]. Hamzah,1993, Hukum Pidana Yang Berkaitan Dengan Komputer, Jakarta: Sinar Grafika, 1993, pp. 455-462.

[2]. Bambang Sunggono,1994, Metode Penelitian Hukum, (Jakarta:Raja grafindo persada, 1994: 149 – 153)

[3]. Barda Nawawi Arief, 2007, Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, (Jakarta: Kencana Predana Media Group, 2007), hal.24

[4]. Rahardjo,2012, "Cybercrime," [Online]. Available: http://keamananinternet.tripod.com/pengertian-definisicybercrime.html. [Accessed 11 12 2018].

[5]. Creswell, J. W. (2013). Qualitative inquiry and research design: Choosing among five approaches (3rd ed.). Thousand Oaks, CA: Sage.

[6]. Davidson, J. (2012). The Journal Project: Qualitative Computing and the Technology/Aesthetics Divide in Qualitative Research. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 13(2), Art. 15. Retrieved from

[7]. Dye, Thomas R. (2008). “Understanding Public Policy”. 12th Edition. New Jersey: Prentice Hall.

[8]. DeLeon P and L DeLeon 2002, What Ever Happened to Policy Implementation? an Alternative Approach Journal of Public Administration Research and Theory **12** 467-92).

[9]. Edwards III, George C, 1980. “Implementing Public Policy”. Washington DC: Congressional Quartely Press.

[10]. Hariyanto and A. P. U. Siahaan, "Intrusion Detection System in Network Forensic Analysis and Investigation," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 18, no. 6, pp. 115-121, 2016.

[11]. M. Singh, J. A. Husain and N. K. Vishwas, "A Comprehensive Study of Cyber Law and Cyber Crimes," International Journal of IT, Engineering and Applied Sciences Research (IJIEASR), vol. 3, no. 2, pp. 20-24, 2014.

[12]. P. D. M. Gercke,2012, Understanding CyberCrime: Phenomena, Challenges and Legal Response, ITU Publication.

[13]. Peter Stephenson, Investigating ComputerRelated Crime: A Hanbook For Corporate

[14]. Subarsono, A.G. 2005. Analisis Kebijakan Publik : Konsep, Teori, dan Aplikasi. . Yogyakarta : Pustaka Pelajar

[15]. Sutarman, 2007, Cyber Crime Modus Operasinya dan Penanggulangannya, Yogyakarta: LaksBang Press Indo.

[16]. Republic of Indonesia. Law Number 19 of 2016 concerning Information and electronic transactions.