The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

HYBRID POLICING AS AN ALTERNATIVE POLICING MODEL FOR CYBER CRIME THAT OCCURS IN THE COMPUTING ENVIRONMENT AT THE INFORMATION SOCIETY

KISNU WIDAGSO[1], ADRIANUS MELIALA[2] and ZAKARIAS POERBA[3]

[1,2,3]University of Indonesia. Email: kisnuwidagso1@gmail.com

Abstract

The emergence of cybercrime has made it difficult for the police in Indonesia to tackle cybercrime. It can be seen from the increasing number of cybercrimes in Indonesia from 2012 to 2019, especially in fraud and content-related crimes. Through qualitative research using literature review, interviews, and observation methods, the study identified four factors as the cause of the increase in cybercrime in Indonesia. The four factors are, (1) low digital literacy and a wide digital gap in society; (2) limited capability of the police; (3) absence of knowledge management system; and (4) weak community policing practices. By using eight variables in the Ponsaers (2001) framework, the author makes a hybrid policing model, which is an alternative policing model, to overcome the weaknesses of policing practices by opening up opportunities for community participation in tackling cybercrime. This hybrid policing model can be called a dynamic engine in cybercrime policing which has three typologies, namely non-hybrid policing, semi-hybrid policing, and pseudo-hybrid policing.

Keywords: Cybercrime, Police, Policing, Policing Model, Hybrid Policing.

INTRODUCTION

In the development of a new society known as the information society, information becomes an essential resource and is very influential in political, social, and economic change. The information society characterizes a transition period from the modern and industrial era in which the mode of production, exchange, and social capital are increasingly determined through information (Ibrahim, 2009). In the Indonesian context, the information society is identified through the rapid use of information and communication technology. Based on data compiled by the Central Statistics Agency (2019) during 2015-2019, the use of internet access among households and individuals has increased significantly. In line with this, a survey conducted by the Association of Internet Service Providers (APJII) in 2019-2020 found that internet usage penetration in Indonesia has reached 73.7%. There are around 196.71 million Indonesians who have made and used the internet in their daily lives.

Then, the development of the term fourth industrial revolution or industry 4.0 is a contemporary form of the information society. Where all forms of daily life practice rely on information and communication technology. Therefore, the information society provides major changes for modern society, especially today's global economy (Laudon and Laudon, 2004). The information society in the form of industry 4.0 has indeed opened up many opportunities in trying and influencing life and reshaping the social, cultural, and human economic environment (Schwab, 2016). However, several experts identified problems that emerged along with industry 4.0, namely, 1) increasing risks in data protection, algorithmic bias, discrimination,

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

and privacy: 2) the use of high-powered propaganda tools that filled the digital information ecosystem with disinformation, interference, and misrepresentation; 3) it is difficult to determine the responsible party in the event of a loss, due to the many uses of corporate-governed technologies: and 4) it creates a new context for questioning the ethics of innovation that takes it beyond the human level.

In line with the above conditions, the information society can enable the occurrence of cybercrimes. According to Strebe (2006), cybercrime began when the computer itself appeared and was made easier in the mid-1975s when the use of microcomputers and modems became more widespread. In addition, there are certain characteristics in the information society that allow cybercrimes to occur. These characteristics include security features that are not a serious concern or consideration, vendors are more concentrated on efforts to add features and products, information technology consumers are more interested in using the latest products, even though their security has not been proven (Strebe, 2006).

Cybercrime is a unique typology of crime. At least, there are two unique features of cybercrime, namely from the aspect of the target of the crime and the environment in which the crime occurs. According to Newman and Clarke (2002), the target aspect of crime can be explained by a framework that is acronymized as CRAVED – concealable, removable, available, valuable, enjoyable, and disposable (Clarke, 1999; Newman, 2009). Then Newman (2009) added another concept called networking. In addition, cybercrime also has its characteristics in terms of proximity/distance, scale, challenges, and patterns (Brenner, 2010) Proximity/distance refers to the fact that cybercriminals and their victims do not have to be physically close to each other when the perpetrator commits a crime. They can be in a different city, a different state, or a different country. The scale is described as a condition that cybercrime is not a one-to-one crime, for instance, a criminal does not have to focus himself or pay special attention to one victim. Perpetrators can target multiple victims and can commit several forms of crime at one time. Challenges are not seen as an obstacle for cybercrime to be committed, both during the preparation, planning, and implementation processes. Pattern refers to the many factors that then make cybercrime difficult to identify or track, both in demographic and geographical aspects (Brenner, 2010).

The unique characteristics of cybercrime then also give rise to the demands of a unique reaction. There is an awareness that it is impossible to reduce the crime rate to 0 (zero), so policing efforts are then mostly directed at controlling crime so that it reaches or remains within the limits that can be tolerated by the community, one of which is by bringing up cyber policing. Basically, in police functions, the cyber policing unit is no different from policing in general. In addition, cyber policing also exploits information usage and communication technology in carrying out its duties.

In the Indonesian context, the typology of cybercrime has been in Law no. 19 of 2016 concerning amendments to Law 11 of 2008 on Information and Electronic Transactions (ITE). As stated in the regulation, investigations, arrests, inquisitions need to carry out the punishment of cybercrime perpetrators. Referring to Law No. 2 of 2002 concerning the Indonesian National

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

Police, in particular, Chapter III starting from Article 13 to Article 19, policing of cybercrime cases is completely the main domain or responsibility of the Police.

Although the prevention of cybercrime has been regulated in such a way, data sourced from the Cyber Crime Sub-Directorate of Headquarters and Kompas media shows that cybercrime in Indonesia in 2012-2019 still experienced a significant increase. Based on data from the National Cyber and Crypto Agency (BSSN) in January-April 2020, it was recorded that 88,414,296 cyber-attacks occurred in Indonesia. This condition is caused by many factors, which according to Hayward & Yar (2006), include difficulties in the criminal justice system, and the law enforcement model used still assumes that criminal investigations must focus on the physical location of the crime.

Although the policing of criminal cases committed so far have been supported by adequate resources, including system support and information technology, it is still a policing model with computational characteristics in the information society, which contributes to strengthening the characteristics of proximity, scale, and physical constraints and the pattern of cybercrime that occurred. On the other hand, utilizing technology can help carry out investigations and investigations.

However, this effort is not easy to do considering that digital evidence can be easily contaminated, modified, or manipulated, even when a crime is being committed. As a result, the police have often become very dependent on software to track the digital movements of suspects. Then, they often become frustrated when they face jurisdictional issues, the boundaries of the country where the crime has occurred, and the whereabouts of the victim, while those boundaries do not exist in cyberspace (Gaines & Miller, 2021). It is what makes the phenomenon of crime in the cyber world an iceberg phenomenon, where many cases of cybercrime are not reported. Even if they are reported to the police, the case completion rate is still relatively low.

Considering the unique characteristics of cybercrime and the characteristics of cybercrimes that are rife in Indonesia, there is a promising alternative to cyber policing, namely hybrid policing. Hybrid policing was first used by Johnston in 1992 to refer to government-owned agencies or institutions, other than the police, which is interrelated and also have the authority and duty to conduct policing and law enforcement (Johnston, 2005). Hybrid policing itself merely refers to the cooperation or involvement of various elements in the implementation of policing. Hybrid policing is strengthened by systems and information technology, and is supported and collaborated with stakeholders, including victims (De Guzman, 2013; Parnell, 2013; Vladoiu, 2014). Thus, the question is "how can hybrid policing be formed as a model for policing cybercrime cases in Indonesia?"

LITERATURE REVIEW

Policing Model

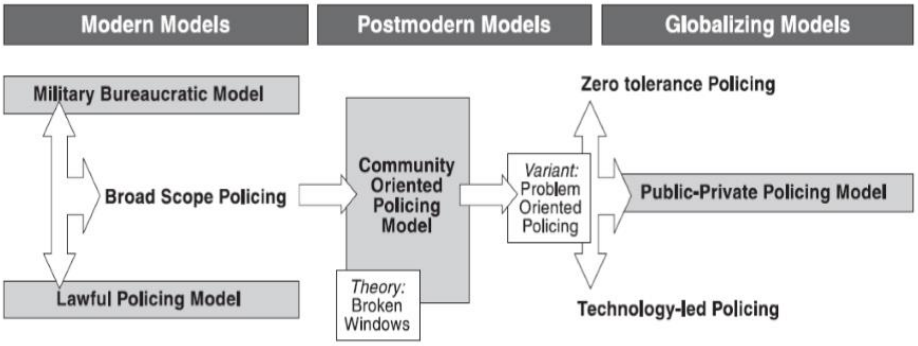
The policing model is a general statement that refers to the orientation and approach of the police in carrying out their main duties or roles. Johnston (1992) uses the concept of a policing

ISSN 1533-9211

DOI 10.5281/zenodo.7432641

model to differentiate the function of the police. With this concept, Johnston (1992) distinguishes the police into 3 (three) typologies, namely reactive force, proactive service, and a combination of the two which Johnston (1992) calls velvet glove and iron fist (Johnston, 1992). According to Ponsaers (2001), until now, there are only 4 (four) models of policing, namely the military-bureaucratic model, the lawful policing model, community-oriented policing (COP), and public-private divide policing. Ponsaers (2001) illustration of the division can be seen as follows:

Figure 1. Policing Model According to Ponsaers (2001)



Source: Ponsaers (2001)

Ideally, referring to Ponsaers (2001), the policing model should be built on 2 (two) principles, namely coherence and normativity and dominance and submission. Ponsaers (2001) also warns that, in practice, the ideal form of a policing model will not exist in the real world. Instead, it is the contamination or osmosis in a policing model. Referring to these two principles, Ponsaers (2001) then operationalizes them into eight variables or factors. They are intended to enable people to see the difference between one policing model and another policing model. The eight variables or factors are:

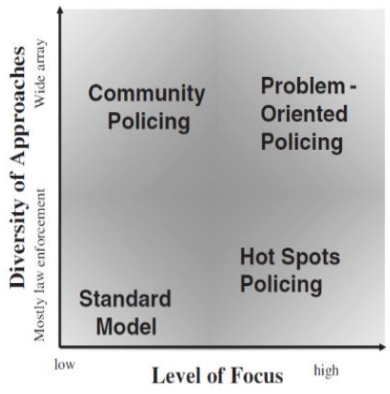
1. Discretion is an authority based on laws and regulations inherent in a person making decisions in carrying out his main duties, especially in conducting investigations and investigating criminal cases.
2. Law as a means, ideally, the existence of laws and regulations is not seen as a goal, but as a means for the police to carry out their main duties and functions.
3. Accountability is a fundamental principle of a democratic society that the police must be held accountable for their actions, interpreted as the responsibility of the police and their policing activities.
4. Relation with the public, the presence of police in the community is to handle emergencies, maintain order, regulate traffic, and promote a sense of security. The police can't perform the tasks or functions alone, but it requires collaboration with the community. On the other hand, police legitimacy is highly dependent on broad and active acceptance and support from the community.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

5. Professionalization, as a background of specific knowledge and skills for the police and the provisions in carrying out their duties.
6. Legitimacy is an acknowledgment from the community on the legitimacy of the policing activities being carried out. The legitimacy of policing efforts will only emerge if the legitimacy is known, interpreted, and understood (read: acknowledgment) by the community. Bjorgo (2016) places the concept of prevention in a broad sense which means reducing the occurrence of criminal acts in the future and reducing the losses caused by the crime itself.
7. Pro/reactiveness, there is a fundamental difference between reactive and proactive nature in policing, which is related to the initiative. The reactive nature of policing can be defined as police responding to specific requests from individuals or groups in the community which includes 'immediate response to calls' and in 'follow-up investigations'. Meanwhile, in proactive policing, the police act on their initiative to develop information about crimes and strategies to suppress these crimes (Weisburd et al., 2019).

Weisburd and Eck (2004) use the concept of a policing model, then differentiate or divide based on the diversity of approaches and level of focus into four policing dimensions, namely standard model, community policing, hot spot policing, and problem-oriented policing in evaluating or assessing the effectiveness of the model. The model in controlling crime and disorder or reducing fear of crime. Illustration according to Weisburd and Eck (2004) of the division can be seen as follows:

Figure 2. Dimensions of Policing Strategy According to Weisburd and Eck (2004)



Source: Weisburd and Eck (2004)

Virtual Community Policing

The concept of virtual community policing is a variant that developed from the concept of community policing. Adler, et.al (2009) define community policing as "… is a model of policing that is decentralized and has officers working with community members to increase feelings of safety in communities" (Adler, et al., 2009). The development of information and communication technology, accompanied by a high level of use by the community, allows the

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

emergence of a new form of community policing that transforms police organizations by creating a virtual police-citizen interface.

Police can easily educate the public about crime in their communities, provide information about police programs, activities, and services, and engage citizens in two-way dialogue. Police can develop profiles on social networking sites, provide a place for social network users to report crimes, enable the public to communicate via text messages with police officers, provide advice and listen to concerns, and provide opportunities for the community to play a role in assisting the police in combating crime (Sirva, 2013).

The virtual police-citizen interface is an innovation in providing good quality and effective police services, as well as creating an environment that allows police to be near and easily accessible in new ways. Virtual community policing can then be defined as:

"Virtual community policing is an interactive means to share and exchange information, to chat and get to know each other and to create trust and confidence in the police. The police also inform people about criminal activities in social media (identity theft, credit card fraud, sexual abuse, wrong identity risks), prevent school bullying, tell children what kind of behaviour is against the law, and give advice (about driving licenses, driving regulations, how to deal with drug dealers, how to report crime online)" (Sirva, 2013).

Hybrid Policing

Hybrid policing was first used by Johnston (1992) without providing a definition. The concept was written as a title in one of the chapters of the book he wrote to refer to the existence of government-owned agencies or institutions, other than the police, which I are interrelate dated and has the authority and duty to conduct policing and law enforcement (Johnston, 1992). The agencies or institutions identified and identified by Johnston (1992) are 1) bodies engaged in functions related to state security; 2) special police forces; 3) departments of state; 4) municipal bodies; 5) miscellaneous regulatory and investigative bodies (Johnston, 1992).

Johnston (1992) emphasized that with the identification of the agency or institution, the study of the police and policing can be further developed considering the concept of hybrid policing is seen as one of the answers to the increasingly diverse forms of crime, such as transportation security, pollution to the environment, nuclear security, international fraud, as well as global terrorism which is on the political agenda. Button (2002), in an article, regarding Johnston (1992), defines hybrid policing as "…embraces all those public bodies (and some private bodies), other than the public police, which is engaged in policing" (Button, 2002). Meanwhile, Manning (2013) defines hybrid policing as "… - this includes all varieties of policing, i.e., noticing, responding to and, perhaps, sanctioning behaviour".

The concept of hybrid policing is also used by Parnell (2013). According to Parnell, hybrid policing is the most effective form of policing in protecting private property rights when state law and policing fail. Parnell defines hybrid policing as "a hybrid form of policing that combines bureaucratic regimentation with the necessity of democratic self-governance" (Parnell, 2013). Regarding the involvement of many elements in policing, although not calling

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

it hybrid policing, Vladoiu (2014) identified the ideal role expected of the parties involved in policing, such as:

1. Government and government institutions, namely to stimulate and control the behavior and process of the transition to the information society by designing specific regulations, frameworks, and action programs.
2. Academic groups, which play a role in building a framework for understanding existing and happening phenomena in the information society, must develop new culture, knowledge, and learning in terms of using technology, and also by developing research, development, and technological innovation.
3. Civil society plays a role in formulating requirements and priorities in the use of new technology for the benefit of the entire community and is responsive to government policies and regulations.

METHOD

Efforts to provide an understanding and explanation of the policing model, most appropriate using a qualitative approach. Because this approach can help provide understanding and explanation in constructing a concept that has some characteristics or characteristics from the real world. These understandings and explanations are dynamic towards social realities and processes (Lave & March 1993; Hayes & Miller, 2006). Then, to obtain data, it is done in three ways, namely:

1. Conducting a literature review of previous research with the keyword model of policing;
2. Conducting observations, carried out by observing the process of policing practices, starting from the emergence of police reports, viewing digital forensic laboratory facilities, attending work meetings, attending socialization about cybercrime in schools, attending seminars on cybercrime, being included in training activities carried out by Interpol in Singapore (September 2017), then accompanied the Interpol delegation on their visit to the UI Faculty of Computer Science (October 2017), helped make the annual report at the end of 2018, attended a talk show on a private television station when discussing Saracen and Muslims Cyber Army (March 2018), until present in the press release of the arrest of perpetrators of cybercrimes;
3. Reconducting unstructured interviews, which were previously conducted on several informants, such as directors, heads of operational subdivisions, heads of sub-directorates, heads of units, and investigators to identify the implementation of practices of policing against cybercrimes. Especially for interviews with investigators, the authors choose investigators who have at least served or served for 1.5 years. The results serve as a reflection of the currently running policing model. At this stage, efforts are also made to look at the obstacles that arise in policing cybercrimes and suggestions or solutions to overcome these obstacles by referring to the characteristics

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

of the community, the weaknesses of the police institution, and the characteristics of cybercrimes. There were also interviews with Ian Walden, an expert on police, policing, and cybercrime.

Technical analysis of qualitative data should assist the process of organizing and sorting data into categories and basic description units, thus, patterns and themes found can be used to guide in conducting analysis (interpretation). In this study, to avoid bias in the analysis, the authors compare the data collected and the data obtained from other studies and compare them with the existing literature. Also, verification is needed to avoid bias, namely by triangulating data. Verification is the author's effort in maintaining the validity of the data used as the basis for the analysis in this study.

Research Proses

The research process consists of several stages. The first stage is to find data on cybercrimes in 2016-2019 handled by the National Police-Criminal Investigation Agency (modus operandi and number). The data date from secondary data, which includes online media news snippets, reports on the results of the analysis and evaluation of the National Police, presentations made by the National Police, as well as the annual reports by the National Police. The data show that online fraud, hoaxes, or hate speech, namely cybercrime, typified as content-related offenses, as well as the production and distribution of illegal content, dominate the modus operandi. In addition, cases of cybercrimes appear, especially those typified as offenses against the confidentiality, integrity, and availability of computer data and systems, which had not been or were not revealed.

The second stage collects data related to the police and policing activities against cybercrimes. In addition to conducting interviews with directors and heads of sections and investigators, the authors also collected secondary data in the form of academic texts on the restructuring of the Polri organization, a book entitled Building a Promoter Dittipidsiber of the National Police-Criminal Investigation Agency, annual reports, and proposals for the development of a Strategic Information and Tactical Operation Center (SITOC). The data show that there are limitations or weaknesses that the police have in policing cybercrimes. The third stage seeks to describe the characteristics of the information technology user community. Utilizing secondary data in the form of research results possibly accessed via the internet help produce the data. These data lead to the finding that Indonesian society has not yet reached the stage in which information technology is available to make meaningful social change, creating something beneficial for humans. The fourth stage interviews Ian Walden, one of the experts who understand the issue of the police, policing, and cybercrime. Walden identified several problems that lead to the weakness of the police in policing cybercrimes, particularly those typified as offenses against the confidentiality, integrity, and availability of computer data and systems. Walden then suggested developing a more suitable policing model for police in policing cybercrimes. The fifth stage is to analyze all existing data findings. Then, the results were narrowed down to the current policing model, considering the existing conditions, the most suitable to be used as a policing model against cybercrime.

ISSN 1533-9211

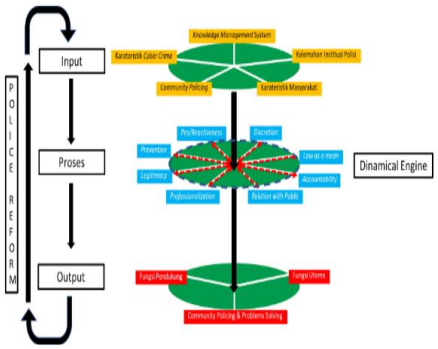
DOI 10.5281/zenodo.7432641

RESULT AND DISCUSSION

For criminology, the police and policing are part of the subject of research, namely as part of an effort to explain the reaction of society in carrying out formal social control against crime and criminals. Criminology also sees the police and policing as a system in action. This paper raises the theme of the policing model which, in essence, is a general statement concerning the orientation and approach of the police in carrying out their main duties or roles. In the context of criminology, the policing model is proposed in a framework that explains informal structures and relationships, by providing an understanding of situations and conditions apart from the police force. The policing model in this paper is the result that will be explained after getting the understanding of a crime, of the use of technology by the community, and of the weaknesses that exist in the police and their policing practices.

Considering the characteristics of cybercrimes that take advantage of opportunities from technological developments, it is necessary to bring up various dynamic social reaction practices, keeping pace with the existing changes. Changes were made to the style of policing, as well as to the basic aspects of the police. Therefore, the police as a future-oriented organization needs to carry out progressive reform by changing their policing model. This is what the cyber police in Indonesia seem to be doing. Thus, the discussion in this paper will refer to the explanation of the hybrid policing model as a dynamic engine in cybercrime policing, as in the following framework:

Figure 3. Hybrid Policing Model as a Dynamic Engine in Cyber Crime Policing



Source: Edited by the author, referring to the Ponsaers (2001) framework

Factors as Inputs in the Policing Model

The police model in policing to deal with cybercrimes occurring in Indonesia needs changes. The necessity to respond to the existence of conditions requires some changes in the policing model, namely five circumstances called factors as inputs to the policing model. First, regarding the characteristics of cybercrimes handled by the police, most of which are cybercrimes typified as content-related offenses, production, and distribution of illegal content in the digital environment, without the appearance of data corruption, information, or computer systems. The police are required to handle or uncover cybercrimes typified into offenses against the confidentiality, integrity, and availability of computer data and systems.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

Second, changes to the policing model are based on the characteristics of the information technology user community. In the context of Indonesia, users of information technology have not yet reached the perfect level or quadrant of the computing environment and information society. Currently, Indonesian people do not understand the stage of information technology exploitation to make meaningful social changes, creating something beneficial for humans (Olsen, et al. (Eds.), 2009). This condition exists due to the lack of knowledge of information technology users about the rules and norms in interacting online in the digital landscape (Leogrande, 2014). The perpetrators of spreading hoaxes and hate speech, for example, do not understand that their behavior is a violation of the concept of digital etiquette or netiquette, they do not understand that their behavior is closely related to digital rights and responsibilities, and the existence of laws and regulations that criminalize his behavior (Law of the Republic of Indonesia No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE)). In addition, there is also the fact that Indonesia is also experiencing the digital divide phenomenon.

Third, it refers to the limitations or weaknesses of the police in policing cybercrimes. The police respond to this limitation by providing a managerial approach to managing the organization. The police carefully calculate and manage to meet the needs of the organization's resources, such as people and budgets, to develop certain policing methods, as well as to meet the availability of facilities and infrastructure. From 2016 to 2018, in terms of quantity, the need for organizational resources started to improve by having some changes in the organizational structure, to increase the number of members and send more members to attend training abroad, as well as to increase the budget to meet the need for equipment and maintenance. However, from the police side, the improvements made are always not enough and inadequate. The increasing number of cybercrime cases (meaning a lot of budgets are needed for inquiries and investigations) and the high cost of equipment maintenance always serve as the two components leading to insufficient budget provided by the government.

Fourth relates to the existence of a knowledge management system (KMS) owned by the police. Knowledge is important for policing activities, considering that knowledge contains laws and regulations governing crimes and violations of the law, evidence, legal precedents, and police conduct rules, and information that needs to be shared with all members of the organization. During field observations, this KMS was not found in its ideal form. Knowledge about policing against cybercrime is stored in each member so that when a member rotation or mutation occurs, knowledge then moves and even becomes lost.

Fifth is the implementation of community policing practices by the police. In cybercrime policing, the police seem to have shifted to a more proactive nature, for example cooperating (collaborating) with e-commerce, public institutions, as well as utilizing social media. Involving business institutions with sustainability also seems to play a strategic function in the established cooperation. Business institutions, especially companies known to be the hosts of cybercriminals, can be involved in preventing cybercrime (Bell, 2014), including having adequate standards of decency and information security. However, the changes in organizational structure and work procedures that confirm the existence of the Directorate of

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

Cyber Crimes cannot be seen as part of the transformation organization within the framework of community policing. The increase in the number of members and the budget has not been in line with the visible allocation of the organization's resources to establish relations with the crime-prevention-oriented community. The entire organization's resources are still focused on orientation to law enforcement, investigation efforts, and cybercrime investigations.

Aspects in the Dynamic Process of Establishing a Policing Model

The Policing Model of Cyber Crime from the Police Perspective

There are eight aspects given by Ponsaers (2001) and need to be studied to identify the policing model. This context will explore the current model of policing. The first is discretion, where as far as field observations are concerned, this aspect of discretion lies entirely and becomes the authority of investigators whose technical accountability is carried out in stages, starting with the head of the unit, the head of the sub-directorate, up to the director. For cybercrime cases that are considered complex or severe, accountability is carried out through a case title mechanism attended by investigation supervisors and representatives from the profession and security sector. Almost the entire process is initiated, implemented, and supervised by the police. In the field observations, the suspect or victim is rarely seen getting involved in this series of processes. If later there are parties who object to the decisions made, they can file a pretrial.

The second is the aspect of law as a means. In this context, the laws and regulations do not function as an objective, but as a means of carrying out the main duties and functions for the police. However, in practice, not all activities carried out by the police have guidelines in the form of laws and regulations, thus making policing efforts vulnerable to questioning. In the field observations, this can be seen, for example, in the context of confiscation, retrieval, collection, and storage of digital evidence. At the 2019 Criminal Investigation Agency (Bareskrim) Technical Working Meeting, a draft was made by the Directorate of Cyber Crime regarding the technical regulations, complete with standard operating procedures. The draft was discussed and discussed in a technical meeting by the Special Crime Directors, agreed upon, and then submitted to the Head of the Criminal Investigation Unit of the National Police for the issuance of regulations. Again, the whole process involves only the police.

The third is accountability or the responsibility of the police and their policing activities. In this regard, there are several contexts. First, when carrying out policing duties, the accountability shows up in stages ranging from the head of the unit, the head of the sub-directorate, to the director. Second, in the budgeting context, accountability is carried out in tiers. In addition, the budgeting fulfills financial accountability, which must be submitted to the planning and administration department. In this case, accountability, both in policing activities and in the use of the budget, is only carried out by the police themselves without involving other external parties.

Fourth, namely relations with the public, in policing cybercrimes, this aspect is ideally realized by implementing community policing practices accompanied by the application of a knowledge management system (KMS). Unfortunately, due to several constraints, this did not work.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

However, the police are making efforts to relate to the community by taking advantage of the existence of public relations (which incidentally is also the police) and the involvement of the mass media, namely through press release mechanisms and news coverage by the mass media. The weakness is that the relationship that is formed is a one-way relationship, which only shows the disclosure of cybercrime cases that are of public concern, a very thick description from the perspective of the police, and with a limited duration.

The fifth aspect is professionalization, which is in this simple term as background knowledge and skills specific to the police equipped in carrying out their duties. Based on field observations, not all cybercrime investigators have background knowledge and skills in information technology. Knowledge and ability in policing cybercrimes are generally present along with their involvement as cybercriminal investigators.

Legitimacy, as the sixth aspect, is simply translated as an acknowledgment from the community of the legitimacy of the policing activities carried out. In the opinion of the police, this legitimacy is considered to have been achieved by showing and confirming to the public that the policing activities carried out are under the criminal procedure law, the collection of valid evidence, the fulfillment of the criminal element, and having passed the case process (usually submitted through the press releases). The whole process is carried out by the police without involving outsiders.

The seventh aspect is prevention, where ideal prevention efforts can be achieved if the police can develop community policing practices accompanied by the application of a knowledge management system (KMS), as well as that the police can act as a pressure group for the government to make macro public policy improvements. to reduce cybercrime. However, the police's understanding appears to be limited. The police still believe that law enforcement will have deterrence effects, especially secondary deterrence, the public will not commit cybercrimes.

Pro/reactiveness, as the eighth aspect, can be translated as police tactics or tactics in controlling crime. In the author's view, the determination of tactics is often not based solely on increasing the number of reported crimes or referring to the needs of the community, but rather is the result of situation definition, understanding, and police decisions by referring to the analysis they make of the contemporary situation. Even in certain contexts, leadership policies become the dominant element in determining policing tactics. This can be seen, for example, at the time of the regional elections, the election of members of the legislature, and the presidential election. The police then defined that lies and hate on social media were a threat to democratic elections, and subsequently, the police formed a social media task force and developed cyber patrols.

Thus, the explanation of the eight aspects in the dynamic process of forming the policing model has shown that none of the aspects are played by parties outside the police. Even if there are, apparently, they exist only in small proportions. This shows a strong characteristic of monopolistic policing in policing cybercrimes in Indonesia. Maybe this model is currently considered suitable for policing cybercrimes, but we should keep in mind that this model has a

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

vulnerability to abuse of power by the police which in fact cannot solve the existing pile of cybercrime cases.

Policing Model According to Cyber Policing Exper

Data collection was also carried out for Walden, in the context of this paper, the data obtained were interpreted and then formed into a policing model against cybercrime while staying within the framework proposed by Ponsaers (2001). In the data findings, Walden has indirectly mentioned that the police must develop a policing model with the nuances of hybrid policing which is starting to be felt. Walden used a dynamic process as a reference in the formation of a policing model, it appears that first, there is a division of authority and responsibility between the government and the police in dealing with cybercrime cases. Second, the limited discretion given to the police is only allowed for cybercrimes which are offenses against the confidentiality, integrity, and availability of computer data and systems, especially those that threaten critical national infrastructure. Third, in the aspect of law as a means, the entire regulatory framework required for the police to carry out policing work against cybercrimes is established by the government. Fourth, related to the aspect of relations with the public, at least the development of relations with the community is carried out, but it is still encouraged to develop cooperation with the cyber police community in an international scope. Fifth, regarding the accountability aspect, the cyber police are fully accountable for all their policing activities to the government, considering that funding and the laws and regulations that form the basis of policing are the domain of the government's role, as well as demands to maintain critical national infrastructure.

Sixth, related to professionalization, this aspect is the domain of government responsibility manifested in the provision of cooperation for education and training, including recruitment, from law enforcement and information technology experts. Seventh, the legitimacy aspect is achieved by the ability of the police to provide guarantees to the government on the confidentiality, integrity, and availability of critical national infrastructure. Eighth, related to the pro/reactiveness aspect, the decision to carry out this tactic is taken by the police based on an understanding of the development of threats to critical national infrastructure that emerged along with the rapid development of information technology. Lastly, it is necessary to share the prevention aspect between the government and the police. The government implements secondary and tertiary crime prevention, while the police are trying to create general deterrence.

Alternate Policing Models – Hybrid Policing

The previous explanation becomes the basis for forming a policing model with a more pronounced hybrid policing nuance as an alternative and as a form of compromise or adaptation to the situation and conditions of the factors that are input in developing the policing model.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

The explanation is as follows:

1. The discretionary aspect. This discretion has primarily been used ever since the police report to transfer all cases to another unit was received, except for cybercrime cases, which are offenses against the confidentiality, integrity, and availability of computer data and systems. Considering that not all units have the capability, equipment, and facilities to carry out digital forensics, the cyber unit is then required to provide technical assistance. Therefore, in this situation, it is necessary to establish legislation (Regulation of the National Police Chief) that supports the practice of delegation of authority.
2. The aspect of law as a means. The government must provide the legal framework required by the police in policing cybercrimes. If technical regulations are needed, the police must provide opportunities for experts, or information technology universities to discuss and discuss the technical regulations required.
3. The aspects of relations with the public. Implementing community policing by providing or sharing knowledge with the community development unit to include cyber issues in their relationship with the community. The development of a knowledge management system (KMS) can be done together with the information and communication technology unit of the police at headquarters or the regional police, apart from having to share authority with public relations.
4. The accountability aspect. It is the accountability for using the budget internally to the government and the public by making annual reports that are made periodically and then published widely.
5. The aspect of professionalization. Members in the cyber unit must have an information technology background or have undergone cyber education or training. To strengthen this aspect, it is possible to involve or invite any experts or experts in the field of information technology (not in the capacity as expert witnesses), in particular, to be involved in the digital forensic process and assessment of the quality of digital forensic results.
6. The aspect of legitimacy. The police have a desire to open up space for public involvement, such as in the process of inquiry and investigation, to generate public support for the police and policing.
7. The aspect pro/reactiveness. The police must base the tactics on understanding the reports made by the cyber community, the results of the analysis of cybersecurity experts and academics, and even the results of research conducted by information system security companies, both at home and abroad.
8. The prevention aspect. Police should use community development and public relations units to convey crime prevention messages, including sharing this role with cyber communities and academics.

This alternative model is not by nature a perfect hybrid policing. However, this model at least shows that in every aspect of the dynamic process of establishing a policing model, in essence, it is not something that should be a monopoly of the cyber police. Every aspect of this dynamic

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

process can be shared with other parties, whether within the police institution itself, the government, or the community.

By using hybrid policing as a model, the writer also finds that if all aspects of the dynamic process are monopolized by the police, it can be said as a typology of non-hybrid policing. Then, the explanation from the expert who suggested that the police should be able to assist or release some aspects of the dynamic process of forming a policing model to other parties can refer to as semi-hybrid policing. Meanwhile, as a form of compromise or adaptation to the situation and conditions of the factors that are input in developing a policing model and expert explanations, a model can be developed where there is a release of dynamic aspects to other police units but is still part of the police force. In this context, it can be typified as pseudo hybrid policing.

CONCLUSION

Cybercrime has become one of the characteristics that emerged along with social changes occurring in society. This change seemed to be responded to by the police with stuttering and unpreparedness. Seeing cybercrime data and cybercrime cases arrears is a symptom that must be responded to by making changes to the policing model. Some conditions are then referred to as factors as inputs in the policing model, which further strengthen the basis of the development of a policing model. Furthermore, by borrowing the framework offered by Ponsaers (2001) the researcher has operationalized eight aspects in the dynamic process of forming the policing model. Aspects that then become complete and comprehensive can be used to develop a policing model against cybercrime.

Therefore, the policing model later referred to is hybrid policing. Hybrid policing is a strong candidate as the basic foundation for developing a policing model with consideration that this policing model is seen as an answer to the increasingly diverse forms of crime, can overcome the weaknesses of the police, and promises to be able to conduct policing more effectively. This model also opens the opportunity for the community to have or be given the authority, which has been owned by the police, in conducting policing.

ACKNOWLEDGMENTS

The author (s) thank you for the funding provided through the Universitas Indonesia Final Doctoral Student Grant (TADOC) 2018.

References

- Adler, F. (2009). Criminology. The McGraw-Hill Companies.
- Bjorgo, T. (2016). Preventing Crime: A Holistic Approach. London: Palgrave Macmillan.
- Brantingham, P. J., & Brantingham, P. (2001). The Implications of the Criminal Event Model for Crime Prevention. The Process and Structure of Crime: Criminal Events and Crime Analysis, 9, 227-303.
- Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. ABC-CLIO.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

- Broadhurst, R. (2006). Developments in the Global Law Enforcement of Cyber-Crime. Policing: An International Journal of Police Strategies & Management.
- Button, M. (2002). Private Policing. Willan Publishing.
- Calder, A. (2005). A Business Guide to Information Security: How to Protect Your Company's IT Assets, Reduce Risks and Understand the Law. Kogan Page Publishers.
- Chandra, A., & Snowe, M. J. (2020). A Taxonomy of Cybercrime: Theory and Design. International Journal of Accounting Information Systems, 38, 100467. https://doi.org/10.1016/j.accinf.2020.100467.
- Clarke, R. V. G., & Webb, B. (1999). Hot products: Understanding, Anticipating and Reducing Demand for Stolen Goods (Vol. 112). London: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate.
- Council of Europe. (2003). Additional Protocol to the Convention on Cybercrime. Article 6.1 Concerning The Criminalisation of Acts of A Racist and Xenophobic Nature Committed Through Computer Systems. Strasbourg: Council of Europe.
- Council of Europe. (2020). Chart of Signatures and Ratifications of Treaty 185. Convention on Cybercrime. https://www.coe.int/en/web/conventions/full-list/ /conventions/treaty /185/signatures?p_auth=XkyltBzP.
- De Guzman, M. C., Das, A. M., Das, D. K., & De Guzman, M. C. (2013). Evolution of Policing. Crc Press.
- Gaines, L. K., & Miller, R. L. (2021). Criminal Justice in Action. Cengage Learning.
- Greene, J. R. (2007). The Encyclopedia of Police Science (Vol. 1). Taylor & Francis.
- Harvey, K. (Ed.). (2013). Encyclopedia of Social Media and Politics. Sage Publications.
- Hayes, B, & Miller, R. (2006) Modeling. In Turner, Bryan S (Ed.). The Cambridge dictionary of sociology. Cambridge University Press.
- Hayward, K., & Yar, M. (2006). The 'Chav' Phenomenon: Consumption, Media and the Construction of a New Underclass. Crime, Media, Culture, 2(1), 9-28.
- Ibrahim, Y. (2009). Technology Discourses in Globalization Debates. In Encyclopedia of Information Science and Technology, Second Edition (pp. 3700-3706). IGI Global.
- Innes, M. (2003). Understanding Social Control. McGraw-Hill Education (UK).
- Johnston, L. (2005). The Rebirth of Private Policing. Routledge.
- Johnston, L. E. S. (1992). The Politics of Private Policing. The Political Quarterly, 63(3), 341-349.
- Laudon, K. C., & Laudon, J. P. (2004). Management Information Systems: Managing the Digital Firm. Pearson Educación.
- Lave, C. A., & March, J. G. (1993). An Introduction to Models in the Social Sciences. University Press of America.
- Leogrande, C. (2014). Education, Issues in. In Harvey, Kerric (Ed.). Encyclopedia of social media and politics. Sage Publications, Inc.
- Levi, M., & Williams, M. L. (2013). Multi-Agency Partnerships in Cybercrime Reduction: Mapping the UK Information Assurance Network Cooperation Space. Information Management & Computer Security.
- Lipton, J. D. (2011). Combating Cyber-Victimization. Berkeley Tech. LJ, 26, 1103.
- Manners-Bell, J. (2014). Supply Chain Risk: Understanding Emerging Threats to Global Supply Chains. Kogan Page Publishers.

The Seybold Report
ISSN 1533-9211
DOI 10.5281/zenodo.7432641

- Manning, P. K. (2013). Policing: Privatizing and Changes in the Policing Web. In The future of policing (pp. 23-39). Routledge.
- Newman, G. R. (2009). Cybercrime. In Handbook on crime and deviance (pp. 551-584). Springer, New York, NY.
- Newman, G., & Clarke, R. V. (2002). Etailing: New Opportunities for Crime, New Opportunities for Prevention. HM Stationery Office.
- Olsen, J. K. B., Pedersen, S. A., & Hendricks, V. F. (2009). A Companion to the Philosophy of Technology. Blackwell Publishing Ltd
- Parnell, P. C. (2013). Policing Private Property against Poverty in Metropolitan Manila. In Policing and Contemporary Governance (pp. 207-230). Palgrave Macmillan, New York.
- Ponsaers, P. (2001). Reading about "Community (Oriented) Policing" and Police Models. Policing: an International Journal of Police Strategies & Management.
- Sallavaci, O. (2017, January). Combating Cyber Dependent Crimes: The Legal Framework in the UK. In International Conference on Global Security, Safety, and Sustainability (pp. 53-66). Springer, Cham.
- Schwab, K. (2016). The Fourth Industrial Revolution. The Cambodian Journal of International Studies, 65.
- Shah, M. H., Jones, P., & Choudrie, J. (2019). Cybercrimes Prevention: Promising Organisational Practices. Information Technology & People.
- Shinder, D. L., & Cross, M. (2008). Scene of the Cybercrime. Elsevier.
- Strebe, M. (2006). Network Security Foundations: Technology fundamentals for IT Success. John Wiley & Sons.
- Strikwerda, L. (2014). Should Virtual Cybercrime be Regulated by Means of Criminal Law? A Philosophical, Legal-Economic, Pragmatic and Constitutional Dimension. Information & Communications Technology Law, 23(1), 31-60.
- Virta, S. (2013). Finland. In Nalla, Mahesh K. & Newman, Graeme R. (Eds.), Community policing in indigenous communities. CRC Press.
- Vlădoiu, N. M. (2014). An Analytical Overview on the Virtual Environmental Crime. Law Review, 4(1), 8-16.
- Walden, I. (2005). Crime and Security in Cyberspace. Cambridge Review of International Affairs, 18(1), 51–68. https://doi.org/10.1080/09557570500059563.
- Walden, I. (2018). 'The Sky is Falling!'–Responses to the 'Going Dark' problem. Computer Law & Security Review, 34(4), 901-907.
- Walker, S. (2006). Police Accountability: Current Issues and Research Needs. Washington: National Institute of Justice (NIJ) Policing Research Workshop: Planning for the Future.
- Weisburd, D., & Eck, J. E. (2004). What Can Police do to Reduce Crime, Disorder, and Fear?. The Annals of the American Academy of Political and Social Science, 593(1), 42-65.
- Weisburd, D., Majmundar, M. K., Aden, H., Braga, A., Bueermann, J., Cook, P. J., & Tyler, T. (2019). Proactive Policing: A Summary of the Report of the National Academies of Sciences, Engineering, and Medicine. Asian Journal of Criminology, 14(2), 145-177.