Vegueta. Anuario de la Facultad de Geografía e Historia
23 (1), December 2023
eISSN: 2341-1112

INTELLIGENCE-LED POLICING THROUGH COMMUNITY POLICE COLLABORATION IN RESOLVING CYBER CRIME CRIME CASES

Ilham Urane [1] , Suryadi MT [2] , Muhammad Erza Aminanto [3]
[1,3] Graduate School of Strategic and Global Studies, Universitas Indonesia
[2] Department of Mathematics, Universitas Indonesia
Email: ilham.urane@ui.ac.id ; yadi.mt@sci.ui.ac.id ; erza.aminanto@ui.ac.id

Abstract
This research aims to investigate and analyze the application of the Intelligence-led Policing (ILP) approach through community police collaboration in resolving cyber crime cases. ILP is a policing strategy that integrates artificial intelligence and data analysis into police operational decisions. This research uses a qualitative approach with descriptive methods. The research results show that cyber crime in Indonesia, which is anonymous, international and persistent, is a major concern for the National Police. In response to this challenge, the Dittipidsiber Bareskrim Polri was formed with a commitment to crack down on and prevent cybercrime through an Intelligence-led Policing (ILP) approach. The implementation of ILP is supported by community-oriented policing as a proactive effort to collect essential data and information. Partner cooperation programs, both at the internal and external levels, are the main strategy in dealing with cyber crime. Dittipidsiber Bareskrim Polri also collaborates at the national and international levels, adopts the ILP strategy, and carries out capacity building through global partnerships. This holistic approach aims to improve responses to cybercrime, maintain order and prevent cybercrime more effectively.
Keywords: Intelligence-led policing, Cybercrime, National Police, Community Police

A. INTRODUCTION

Over the last decade, technological development has reached its peak, especially with the Covid-19 pandemic which has pushed society's dependence on Information and Communication Technology (ICT) (Pasculli, 2020). This has led to a significant increase in cybercrime, reaching global losses of approximately US$6 billion in 2021, with 4.1 billion accounts experiencing data leaks in 2019 (FBI, 2021). The State Crypto and Cyber Agency (BSSN) notes that cyber crime in Indonesia continues to increase, reaching more than 100 million cases by mid-2022 (Andreya, 2022). The types of cybercrime that have dominated over the past six years involve gambling, insults, threats and extortion, with thousands of public complaints for each category. (Cyber Police, 2023).

In addition to the previously mentioned categories of cyber crime, various other criminal acts have also been reported to the Cyber Police over the last six years. These figures represent officially recorded complaint data, so it is likely that the actual number of cyber crimes in Indonesia is much higher if unreported cases are taken into account (Pusiknas Polri, 2023). This fact confirms that Indonesia is still vulnerable to the threat of

**Autora de correspondencia / Corresponding author.*

cyber crime, and effective handling by the authorities is crucial (Babys, 2021). Cybercrime in Indonesia is a serious challenge for the government, so regular evaluations are carried out to ensure effective enforcement and prevention measures. This evaluation and development process is not only carried out by the Ministry of Communication and Informatics (Ministry of Communication and Information), but also by the police as the authorized institution that receives public reports regarding cyber crimes (Yunus, 2020).

However, the complexity of the challenges in cracking down on and preventing cybercrime is not only based on the complexity of the technology itself, but also lies in the challenges to the authorized bodies that handle it (Wahyuni, 2018). Currently, in dealing with cyber crime, the police still use a limited structure to carry out action and prevention (POLRI RI, 2022), where this structure is unable to accommodate all types of cyber crime submitted by the public. In the trend of cyber crime in Indonesia over the last few years, the police, as one of the bodies authorized to deal with crime, is also evaluating its structure in order to improve its ability to meet public demand for dealing with cyber crime, such as the plan to establish a Cyber Crime Directorate in each Regional Police (Polda). POLRI RI, 2022).

In facing the dynamics of digital development, it is important to adopt the Intelligence-Led Policing (ILP) method, which focuses on utilizing information and intelligence analysis to guide strategic and tactical decisions (Jackson & Brown, 20070. This approach aims to optimize resource allocation, increasing efficiency operations, and provide a more effective response to crime and public security problems (Fritsvold, 2009). By utilizing intelligence data and information, ILP provides a solid foundation for the police to understand the dynamics of cyber crime and develop appropriate response strategies.

ILP does not just collect information, but also applies a proactive approach by using data analysis to identify crime patterns and develop smarter response strategies. With the adoption of ILP, police can respond more quickly to digital security threats and increase their responsiveness to the rapidly changing crime environment (Carter, 2016). Therefore, the development and implementation of ILP is an urgent need to ensure efficient and adaptive handling of cybercrime challenges in this digital era.

Intelligence-Based Law Enforcement Empowerment (ILP) not only serves as an additional information center within an organization, but also provides strategic integration of intelligence into the law enforcement organization's overall mission. ILP represents a new dimension of community policing, incorporating tactics and methodologies that have been developed through years of community policing experimentation (Bullock, 2013). In many ways, there are similarities between community policing and ILP, in that both rely heavily on key factors such as information management, two-way communication with the public, data analysis, and problem solving (Ratcliffe, 2016).

A comparison between community policing and ILP shows that both have similar foundations in information management and effective communication with the community. While community policing focuses on developing relationships with communities to understand local needs and challenges, ILP further integrates in-depth intelligence analysis to guide the organization's overall tactical and strategic decisions (McGarrel et al., 2007). As such, ILP can be seen as a more advanced evolution of the concept of community policing, bringing a unique blend of community-based approaches and the use of intelligence to modern law enforcement.

The concept of Intelligence-Led Policing (ILP) began to be implemented in some metropolitan police departments in the United States following the terrorist attacks on September 11, 2001. As time went by, the

practice of ILP grew, and many smaller and medium-sized police departments began to form enforcement units. laws based on their own internal intelligence. In response to the events of 9/11, the New York Police Department (NYPD) created a counter-terrorism unit and organized its intelligence division, which later became the NYPD Intelligence Bureau. The primary mission of the NYPD Intelligence Bureau is "to detect and disrupt criminal and terrorist activity through the use of intelligence-based law enforcement empowerment" (Fritsvold, 2023).

These steps marked a paradigm shift in law enforcement in the United States, with greater emphasis on leveraging intelligence to address criminal and terrorist threats. These ILP units not only operate at the national level, but also at the local level, allowing smaller police departments to adopt strategies that have proven effective in dealing with crime and threats to public safety. Through the implementation of ILP, police departments in the United States are creating responsive and adaptive structures to address evolving security challenges (Fritzvold, 2023).

This research aims to increase the effectiveness of law enforcement against cyber crime by analyzing the implementation of Intelligence-Led Policing (ILP) through community police collaboration. The aim is to understand how ILP, especially involving community police, can be optimized to deal with cybercrime more efficiently. The main benefits of this research include improving law enforcement responses to cybercrime, optimizing resource allocation, developing cyber security strategy models, and increasing public awareness of the role of ILP and community police in preventing and controlling cybercrime. It is hoped that the research results can make a practical contribution in improving law enforcement capabilities and public awareness regarding cyber security.

B. METHOD

This study uses a qualitative method. Creswell & Poth (2016) state that qualitative research begins with assumptions and the use of an interpretive/theoretical framework that informs the study of research problems addressing the meaning individuals or groups ascribe to social or human problems. Following the approach above, the author uses descriptive analysis methods in this research. This clarifies the situation and problems that were being carried out at that time. Descriptive analysis is a study that aims to describe or explain something as it is (Yulianah, 2022). Therefore, descriptive research does not provide testing of a particular hypothesis, but only explains what the variables, symptoms and situations are (Irawan, 2006). This research was conducted at the Directorate of Cyber Crime, Criminal Investigation Agency of the Republic of Indonesia Police. The research that will be carried out will take one year, starting from January 2023 to December 2023. The data collection technique is carried out using documentary interviews and observation. Next, the collected data is validated through the triangulation method to collect existing data and sources as well as view, check and test the credibility of the data obtained. Next, the data will be analyzed using data analysis using the Miles & Huberman (1984) approach.

C. RESULTS AND DISCUSSION

The community-oriented policing approach is a crucial aspect in prosecuting cybercrime, as expressed by Skogan & Harnett (1997) with the main concepts focusing on community, partnership and decentralization. This approach allows the police, especially the Dittipidsiber Bareskrim Polri, to become multi-functional and

provide services and responsibilities at the grassroots level. In the context of prosecuting cybercrime, the proactive approach of Dittipidsiber Bareskrim Polri is the main result of implementing intelligence-led policing (Tilley, 2012).

This proactive nature is essential to support a rapid and effective response to the ever-evolving cybercrime threat. Apart from that, community-oriented policing is also considered to be able to reduce weaknesses in the hybrid policing pattern carried out by the Dittipidsiber Bareskrim Polri, especially in the aspect of crime clearance. By integrating work units (satker) that specialize in handling cyber crimes, this approach helps overcome overlap with other working units that handle conventional crimes. Even though cyber security often overlaps with other work units, the implementation of community-oriented policing can increase focus and effectiveness in tackling cyber crime within the National Police's internal environment.

The importance of information management and two-way communication with the public is a crucial element in optimizing the intelligence-led policing approach, as stated by Ratcliffe (2016). Dittipidsiber Bareskrim Polri implements intelligence-led policing through three main ways, namely collaborative partnerships (partnership programs), capacity building (capacity building), and Netizen Police. These three programs have similar objectives, namely collecting data and information related to cyber crime from the public through two-way interaction. Through this communication, Dittipidsiber Bareskrim Polri seeks to build active involvement with the community to gain a better understanding of the threat of cyber crime.

The partnership program aims to increase cooperation with related parties outside the police, while capacity building focuses on increasing internal capabilities to face and overcome cyber crime. Netizen Police, as one of the initiatives, represents an effort to create a police presence in cyberspace, gather information from netizens, and raise public awareness about cybercrime. All of these programs support the collection of data and information originating from the community through two-way dialogue, then the data is processed and analyzed to form preventive, responsive and preemptive handling strategies for cyber crime. With this approach, Dittipidsiber Bareskrim Polri seeks to build a solid foundation for handling intelligence-based cyber crimes.

.**Table 1**

Intelligence-led Policing Model Strategy at National and International Levels

Policing Type	Levels	Strategy	Partner
Intelligence-led policing	National	a. Partnership collaboration (partnership program) b. Netizen police c. Capacity building (capacity building)	a. Internal: All National Police Units External: Government (ex. BSSN, Ministry of Defense, Coordinating Ministry for Political, Legal and Security Affairs, Kominfo) b. Public; Cyber influencer c. External and internal police
	International	a. Partnership collaboration (partnership program)	a. United States, European countries; Interpol and Europol b. Interpol, Europol

		b. Capacity building (capacity building)	

Source: Yunus (2020)

In an optimal effort to deal with cyber crime at the national and international levels, Dittipidsiber Bareskrim Polri prioritizes partnership cooperation strategies as the first step. This strategy is based on the concept of community-oriented policing, which focuses on close relationships between the police and the community in order to improve environmental quality (Ponsaers, 2001). In addition, this approach also reflects the focus of community-oriented policing identified by Skogan & Harnett (1977). The link between community-oriented policing and intelligence-led policing arises from the operational needs of the police which require comprehensive data and information.

The implementation of this strategy illustrates the active involvement of Dittipdsiber Bareskrim Polri with the community and society in collecting information related to cyber crime. Through proactive cooperation and assistance from external parties, especially the community, law enforcement can access more necessary data and information. This approach is the key to conducting in-depth analysis to identify patterns of crime that may not have been detected through the implementation of smart policing. By building a solid foundation of cooperation, Dittipdsiber Bareskrim Polri seeks to create an environment where information can be exchanged effectively to increase the success of law enforcement strategies against cybercrime.

In an effort to increase external cooperation at the national level, Dittipidsiber Bareskrim Polri has established partners with various institutions and agencies, including the National Cyber and Crypto Agency (BSSN), the Coordinating Ministry for Political, Legal and Security Affairs (Kemenko Polkuham), the Ministry of Defense (Kemenhan), and Ministry of Communication and Information (Keminfo). This collaboration indicates that there is synergy between law enforcement agencies and the government in tackling cyber crime at the national level. Apart from that, Dittipidsiber Bareskrim Polri also collaborates with the private sector and the community to participate in this collaboration, creating an inclusive platform that involves all elements of society.

At the national level, the Netizen Police program is a concrete effort to involve the public and the private sector in efforts to suppress cyber crime. This program reflects awareness of the important role of society in gathering information related to cybercrime. Involving the private sector also shows that collaboration with the industrial sector is a crucial step in overcoming the threat of cyber crime. By integrating various parties, Dittipidsiber Bareskrim Polri aims to create strong synergy to support holistic and optimal handling of cyber crime at the national level.

Netizen police involving influencers in the cyber world, which are categorized as Ring I, Ring II and Ring III, are an important element in the cyber crime suppression strategy. These influencers, with significant followings, have the potential to bring greater attention to cybercrimes. The categorization in Ring levels reflects the level of influence and reach of each influencer, so that collaboration with them can be an effective means of voicing cybersecurity issues.

The positive influence of the relationship between netizens and the police, especially through influencers, not only creates public awareness of the threat of cybercrime, but also allows for increased active participation in crime reporting. This is in accordance with the concept of intelligence-led policing through

community-oriented policing which emphasizes two-way communication (Ratcliffe, 2016). Effective communication between the police and netizens creates a synergistic dynamic where information can be exchanged more quickly and accurately. By involving netizens and influencers, Dittipidsiber Bareskrim Polri creates a strong foundation to support intelligence-led policing strategies in tackling cyber crime responsively and proactively.

By utilizing a 'viral' strategy, Dittipidsiber Bareskrim Polri was able to increase the amount of data and information received significantly. This approach enables widespread and rapid dissemination of cybercrime-related information through various social media platforms and online channels. Apart from obtaining information from the public and netizens, the National Police can also explore and develop data and information obtained from perpetrators of cyber crimes, providing deeper insight into the modus operandi and criminal networks.

Management of data and information received is carried out through three main steps. First, data collection is carried out in a structured and systematic manner, involving various sources such as public reports, information from influencers, and analysis of online activities. Second, data integration enables the unification of diverse information obtained from various sources, creating a more comprehensive understanding of the scope and dynamics of cybercrime. Finally, data analysis is carried out to extract patterns and trends that can help in identifying targets, modus operandi and perpetrators of cybercrime. In this way, Dittipidsiber Bareskrim Polri can manage information more effectively and formulate more appropriate and responsive handling strategies.

In the initial stage, the information management system implemented by Dittipidsiber Bareskrim Polri will actively collect data and information originating from netizens and influencer partners. These reports are considered important in the context of intelligence-led policing, which places great emphasis on data collection and analysis as a basis for effective decision making. After data and information are collected, the next stage involves data integration, where the management system will unite various sources of information into one integrated whole. This step allows the Dittipidsiber Bareskrim Polri to have a more comprehensive view of the dynamics of cyber crime.

Next, in the data analysis stage, an intelligence-led policing approach is used to uncover patterns, trends and potential anomalies in the integrated data. This analysis aims to form predictions of cybercrime behavior which can be the basis for tactical and strategic decision making. This prediction is a key asset in helping Dittipidsiber Bareskrim Polri optimize resource allocation in enforcement efforts. Thus, this information management system not only functions as a data collection tool, but also as an analytical instrument that helps in handling cyber crimes more efficiently and adaptively.

Within the smart policing framework, a series of strategies are implemented, including online crime reporting, digital investigations, adaptation to the Cloud by the police, digital security and identity, and workforce optimization with a mobile-based approach. These smart policing measures utilize the adaptability of digital technology, such as mobile technology, digital data, mobile digital case files, cyber forensics, and intelligence investigations, to tackle crimes in cyberspace which have different motivational, spatial and temporal complexities than crimes in cyberspace. physical world.

The significant difference between smart policing and intelligence-led policing (ILP) approaches via netizen policing lies in the data and information sources used. In ILP, the National Police proactively

collaborates with netizens and influencers, accessing information resources that are not only digital. This creates greater data diversity, involving reports from the public, not just digital data. On the other hand, ILP provides additional contributions in the form of identifying richer data and patterns related to cyber crime, complementing the investigation results resulting from the smart policing approach. By utilizing the advantages of each approach, Dittipidsiber Bareskrim Polri created a holistic approach to deal with cyber crime more comprehensively and efficiently.

The importance of international cooperation in handling cyber crime is a manifestation of the international nature of this crime, where perpetrators are not only limited to Indonesian citizens, but can also come from other countries. Dittipidsiber Bareskrim Polri understands this complexity and has established partnerships at the international level to face these challenges. Boes & Leukfeldt (2017) note that cybercrime has an international nature because it can occur throughout the world in a complex manner and involves various actors from various countries.

Partnerships with international police organizations such as Interpol and Europol are not only part of the partner cooperation program, but also an integral part of building the capacity of Dittipidsiber Bareskrim Polri and all Polri work units in dealing with cyber crimes. In cooperation at the international level, the National Police is involved in bilateral cooperation which involves the exchange of critical information. This exchange of information helps Dittipidsiber Bareskrim Polri to better face the challenges of international cybercrime. Thus, this joint effort not only improves the response to cybercrime globally but also strengthens national capabilities in dealing with this threat.

Through international partnerships, Dittipidsiber Bareskrim Polri implements a capacity building strategy as a proactive step in dealing with cyber crime. This capacity building involves the exchange of information, knowledge, best practices, technology and science related to handling cyber crime. The Indonesian National Police took advantage of this opportunity to study the strategies that have been implemented by the police of several countries in building their capacity.

There are three important aspects in capacity building that are emphasized by Dittipidsiber Bareskrim Polri through international partnerships, namely first, involving cyber volunteers who become an additional force in handling cyber crimes. Second, make large investments in renewable technology to support law enforcement performance in dealing with cyber crime. And third, increasing global partnerships to ensure effective collaboration in facing the threat of cybercrime that crosses national borders. To date, Dittipidsiber Bareskrim Polri has focused on building its capacity through global partnerships, which has become a strong foundation for increasing national capabilities in dealing with cybercrime challenges.

Through strong initiatives in building capacity, Dittipidsiber Bareskrim Polri is able to deepen and improve its strategy in preventing cybercrime more effectively, by relying on predictions based on more accurate patterns and trends. This step provides substantial support for the objectives of Dittipidsiber Bareskrim Polri in policing, namely maintaining order and preventing crime, as stated by Mawby (2012). Collaboration with international partners is not only a form of adaptability, but also the implementation of a community-oriented policing model in fighting cyber crime.

In closing, the continued efforts of Dittipidsiber Bareskrim Polri in strengthening its capacity and establishing international cooperation shows its seriousness in dealing with the increasingly complex dynamics

of cybercrime. With a proactive and adaptive approach, the National Police is not only prepared to face the threat of cyber crime, but also contributes to creating a safer and more secure cyber environment.

D. CONCLUSION

One of the crime cases in Indonesia that is always evaluated periodically by the National Police to obtain more optimal action and prevention strategies is cybercrime. Cybercrime is anonymous, international, repetitive, continuous, through various channels, and can even attack massively. Therefore, through a shared awareness that cyber crime requires action through a special directorate, the Dittipidsiber Bareskrim Polri was formed to commit to taking action against cyber crimes reported by the public by forming a policing model that can effectively crack down on and prevent cyber crime, namely through Intelligence-led Policing. This implementation uses the help of community-oriented policing as a proactive effort in collecting data and information which is important fuel for ILP. Some forms of community policing to support intelligence-led policing are partner collaboration programs at internal and external levels. At the external level, there are national and international levels. At the national level, the strategy carried out by Dittipidsiber Bareskrim Polri is; (1) Internal cooperation, (2) External cooperation with the government, and (3) Netizen police. Meanwhile at the international level, intelligence-led policing is carried out with a strategy; (1) Bilateral external cooperation, and (2) Capacity building through global cooperation.

REFERENCES

1. Andreya, E. (2022, September 22). Antisipasi Bersama Tingkatkan Sistem dan Cegah Serangan Siber. Ditjen Aptika. https://aptika.kominfo.go.id/2022/09/antisipasi-bersama-tingkatkan-sistem-dan-cegah-serangan-siber/
2. Babys, S. A. (2021). Ancaman Perang Siber Di Era Digital Dan Solusi Keamanan Nasional Indonesia. *Oratio Directa (Prodi Ilmu Komunikasi)*, *3*(1).
3. Boes, S., & Leukfeldt, E.R. (2017). *Fighting Cybercrime: A Joint Effort*.
4. Bullock, K. (2013). Community, intelligence-led policing and crime control. *Policing and society*, *23*(2), 125-144.
5. Carter, J. G. (2016). Institutional pressures and isomorphism: The impact on intelligence-led policing adoption. *Police quarterly*, *19*(4), 435-460.
6. Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.
7. FBI. (2021). Internet Crime Report 2021. Retrieved February 6, 2023, form https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
8. Fritsvold, E. (2023, March). Police Media Relations and Social Media Strategies. University of San Diego. https://onlinedegrees.sandiego.edu/police-media-relations-and-social-media/
9. Fritsvold, E. D. (2009). Under the law: Legal consciousness and radical environmental activism. *Law & Social Inquiry*, *34*(4), 799-824.
10. Irawan, P. (2006). Penelitian kualitatif & kuantitatif untuk ilmu-ilmu sosial. *(No Title)*.

11. Jackson, A. L., & Brown, M. (2007). Ensuring efficiency, interagency cooperation, and protection of civil liberties: Shifting from a traditional model of policing to an intelligence-led policing (ILP) paradigm. *Criminal Justice Studies*, *20*(2), 111-129.
12. Mawby, R.I. (2012). Models of Policing. In T. Newburn (Ed.), *Handbook of Policing*. Taylor & Francis.
13. McGarrell, E. F., Freilich, J. D., & Chermak, S. (2007). Intelligence-led policing as a framework for responding to terrorism. *Journal of Contemporary Criminal Justice*, *23*(2), 142-158.
14. Miles, M. B., & Huberman, A. M. (1984). Drawing valid meaning from qualitative data: Toward a shared craft. *Educational researcher*, *13*(5), 20-30.
15. Pasculli, L. (2020). The Global Causes of Cybercrime and State Responsibilities: Towards an Integrated Interdisciplinary Theory. *Journal of Ethics and Legal Technologies (JELT)*, *2*(1), 48-74.
16. Polisi Siber. (2023). *Statistik Pengaduan Masyarakat. PatroliSiber*: -. Retrieved February 6, 2023, from https://www.patrolisiber.id/
17. POLRI RI. (2022, September 16). Website Resmi Polri - Marak Kejahatan Siber. Polri. Retrieved February 6, 2023, from https://polri.go.id/berita-polri/1786
18. Ponsaers, P. (2001). Reading about "community (oriented) policing" and police models. *Policing: an international journal of police strategies & management*, *24*(4), 470-497.
19. Pusiknas Polri. (2023). Kejahatan Siber di Indonesia Naik Berkali-kali Lipat. Pusiknas Bareskrim Polri. Retrieved December 17, 2023, from https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat
20. Ratcliffe, J. H. (2016). *Intelligence-led policing*. Routledge.
21. Skogan, W. G., & Hartnett, S. M. (1997). Community policing Chicago style. New York.
22. Tilley, N. (2012). *Modern approaches to policing: community, problem-oriented and intelligence-led.* In T. Newburn (Ed.), Handbook of Policing. Taylor & Francis.
23. Wahyuni, H. I. (2018). *Kebijakan Media Baru Di Indonesia:(Harapan Dinamika Dan Capaian Kebijakan Media Baru Di Indonesia)*. Ugm Press.
24. Yulianah, S. E. (2022). *Metodelogi Penelitian Sosial*. CV Rey Media Grafika.
25. Yunus, F. (2020*). Polri Era Disruption*. Pustaka Star's Lub.