International Journal of Integrated Science and Technology (IJIST)
Vol.2, No.5, 2024: 374-383

Transformation Strategy: Indonesian National Police in Coordinating Crime in The Digital Era

Yustinus Bowo Dwinugroho
Sespimma Sespim.Lemdiklat POLRI

Corresponding Author: Yustinus Bowo Dwinugroho; bowo190680@gmail.com

A R T I C L E I N F O

Keywords: Indonesian National Police, crime, strategic transformation, digital era, law enforcement

Received : 20, March
Revised : 25, April
Accepted: 29, May

A B S T R A C T

The Indonesian National Police (POLRI) has the authority to handle crimes regulated by several laws, including Law no. 2 of 2002 concerning the National Police of the Republic of Indonesia, which is the basis for carrying out their duties in maintaining security and public order, enforcing the law, and providing protection and services to the community. The digital era has brought significant changes in various aspects of life, including security and law enforcement. Advances in information and communication technology not only open up new opportunities but also give rise to complex challenges such as cybercrime. This article analyzes POLRI's strategic transformation in responding to digital crime challenges. Through organizational restructuring, increasing personnel capacity, adopting advanced technology, and collaborating with various stakeholders, POLRI is trying to tackle cybercrime more effectively. This study uses a normative juridical approach and combines various theories to provide insight into the development of law enforcement in the digital era and the strategies implemented by POLRI in dealing with digital crime.

DOI: https://doi.org/10.59890/ijist.v2i5.1904
ISSN : 3026-4685
https://journal.multitechpublisher.com/index.php/ijist

INTRODUCTION

The Indonesian National Police has the authority to take action against crimes regulated by several laws which form the legal basis for the duties and functions of the police. Law Number 2 of 2002 concerning the National Police of the Republic of Indonesia is the basis used by the POLRI to carry out its duties in maintaining public security and order, enforcing the law, and providing protection, guidance and service to the community (Arif, 2021). The digital era has brought significant changes in various aspects of life, including in the fields of security and law enforcement. Advances in information and communication technology not only open up new opportunities, but also create complex challenges in the form of cybercrime and other forms of crime that utilize technology (Lubis, 2022). Cybercrime, such as online fraud, hacking, identity theft, and the spread of false information, has become a real threat that requires an innovative and adaptive law enforcement approach (Monique et al., 2022). The Indonesian National Police (POLRI), as the front guard in maintaining security and public order, must carry out strategic transformation to face these threats.

In the rapidly developing digital era, technological advances have brought new challenges to law enforcement agencies around the world. The Indonesian police force, in particular, has faced a significant transformation in its approach to dealing with crime due to the widespread influence of digital technology (Wahyudi et al., 2020). This article aims to analyze the strategic transformation of the Indonesian National Police in responding to digital crime challenges. By exploring the proactive steps taken by the Indonesian Police, this paper seeks to provide insight into the development of law enforcement in the digital era and the strategies used to effectively combat digital crime (Nur et al., 2022). The digital era has revolutionized the nature of criminal activity, presenting law enforcement agencies with the daunting task of keeping pace with rapidly evolving technology and sophisticated methods used by cybercriminals (Irfan et al., 2018). As the Indonesian Police continue to adapt to these challenges, it is important to explore the strategies and initiatives they have implemented to effectively combat digital crime.

This transformation includes adjusting the organizational structure, increasing personnel capacity, adopting advanced technology, and establishing a collaborative framework with various stakeholders. In addition, formulating policies that are responsive to the dynamics of digital crime is crucial to ensuring the operational effectiveness of the National Police. Given the complexity and cross-border nature of digital crime, the National Police also needs to strengthen international cooperation and utilize global intelligence networks (Wijaya & Arifin, 2020). Facts in Indonesia show a significant increase in cybercrime incidents in recent years. According to data from the National Cyber and Crypto Agency (BSSN), in 2023, Indonesia recorded more than 1.2 million cyberattacks targeting various sectors, including government, finance and critical infrastructure (Hermawati & Santiago, 2023). Cybercrime in Indonesia is also developing in more sophisticated forms, such as ransomware, phishing, and

Distributed Denial of Service (DDoS) attacks, which require special handling and appropriate strategies.

The National Police, through the Cyber Crime Directorate, Bareskrim, has taken initial steps in facing this challenge by increasing technical and operational capacity. However, there are still obstacles in terms of limited human resources with special expertise in the field of information technology as well as a lack of sophisticated tools and systems to detect and deal with cyberattacks effectively (Irfan et al., 2018). Apart from that, there is still an urgent need to increase digital literacy among the public in order to reduce vulnerability to cybercrime. In the context of international cooperation, Indonesia has joined various regional and global forums and collaborations, such as the ASEAN Cybersecurity Cooperation Strategy and the Interpol Global Complex for Innovation (Sitorus & Amal, 2022). This collaboration provides a platform for exchanging information, technology and strategies in dealing with transnational cybercrime. However, the implementation and synchronization of policies at the national and international levels still requires improvement to make them more integrated and effective.

This paper will explore the specific tools, training and partnerships that the Indonesian Police have utilized to tackle digital crime. Next, we will examine the legislative framework and policies that have been implemented to support the transformation of law enforcement in Indonesia. Through comprehensive analysis, this paper seeks to explain the success of the strategic transformation of the Indonesian National Police in the digital era, thereby providing valuable insights for law enforcement agencies globally.

THEORETICAL FRAMEWORK

The theoretical framework for analyzing the strategic transformation of the Indonesian National Police (POLRI) in response to digital crime incorporates several key theories (Akbar, 2019). Technological determinism explains how advancements in digital technologies drive societal changes and necessitate the evolution of law enforcement strategies. As technology evolves, so does the nature of crime, requiring POLRI to adopt new tools and methods to combat increasingly sophisticated cybercriminals. This theory highlights the critical need for law enforcement to stay ahead of technological trends to effectively address the challenges posed by the digital era (Sani et al., 2022).

Routine activity theory provides insights into the factors that contribute to the occurrence of cybercrime, emphasizing the convergence of motivated offenders, suitable targets, and a lack of capable guardians (Wijaya & Arifin, 2020). The digital era has expanded the number of potential targets and provided anonymity for offenders, making cybercrime more prevalent. This theory underscores the importance of POLRI enhancing its role as capable guardians by improving its technological capabilities, training personnel, and implementing robust policies to prevent and respond to cyber threats (Nuth, 2008).

Institutional theory examines how POLRI must adapt its organizational structure and policies in response to external pressures such as the rising incidence of cybercrime and the need for international cooperation (Irfan et al.,

2018). This adaptation involves reorganizing the police force, increasing technical capacity, and formulating responsive policies to address the dynamic nature of digital crime. The theory illustrates the importance of institutional flexibility and responsiveness in the face of rapidly evolving technological challenges (Ramli et al., 2020). The Public-Private Partnership (PPP) framework highlights the necessity of collaboration between public institutions and private entities in combating cybercrime (Nur et al., 2022). POLRI's strategic partnerships with technology firms, international organizations, and other governmental agencies are crucial for leveraging resources, expertise, and information (Monique et al., 2022). This collaborative approach ensures a more comprehensive and effective response to the complex and multifaceted nature of cybercrime, emphasizing the role of collective efforts in enhancing law enforcement capabilities.

Lastly, cybercrime and cybersecurity theory provides a foundation for understanding the specific types of cybercrimes prevalent in Indonesia and the specialized approaches required to counteract them. It supports the development of comprehensive cybersecurity measures, public digital literacy programs, and international cooperation. By integrating these theories, the strategic transformation of POLRI can be analyzed in a holistic manner, offering valuable insights into how law enforcement agencies can effectively navigate the challenges of the digital era and enhance their capacity to combat digital crime on a global scale.

METHODS

This research adopts a normative juridical legal research method with a library research approach, where the main data source is written documents from secondary data, including primary, secondary and tertiary legal materials (Efendi & Rijadi, 2022). This approach allows researchers to carry out systematic and accurate descriptive analysis of the law enforcement problems being studied. Data analysis is carried out carefully, remains focused on the scope of the problem, and is based on relevant theories or concepts to explain and compare existing data (Ali, 2021). In this research, a case approach and a statutory approach are used to formulate legal definitions by considering the legal principles contained in statutory regulations (Purwanti, 2020). In addition, various views from experts and authors relevant to the issues discussed are also considered. This approach ensures that the resulting legal definition is rooted in recognized legal principles and takes into account various perspectives that can enrich understanding of the problem being researched.

RESULTS

The results of this study highlight the significant strategic transformation undertaken by the Indonesian National Police (POLRI) in response to the rapidly evolving challenges of cybercrime in the digital era. Through a comprehensive approach that includes organizational restructuring, capacity building, technological adoption, and enhanced collaboration both nationally and internationally, POLRI has made substantial strides in adapting to the demands of modern law enforcement. Despite facing ongoing challenges such as resource limitations and the need for improved digital literacy, the proactive measures

and strategic initiatives implemented by POLRI demonstrate a robust commitment to combating cybercrime effectively. This analysis not only underscores the successes and areas for improvement within POLRI but also provides valuable insights for global law enforcement agencies navigating similar digital threats.

Strategic Transformation and Technological Adaptation

The Indonesian National Police (POLRI) has undertaken significant strategic transformations to address the challenges posed by cybercrime in the digital era. This includes adjusting its organizational structure, enhancing personnel capacity, adopting advanced technology, and establishing collaborative frameworks with various stakeholders. The emphasis on technological adaptation is crucial, as cybercrime continually evolves with advancements in information and communication technologies. The integration of sophisticated tools and systems for detecting and combating cyber threats, alongside efforts to increase digital literacy among the public, exemplifies POLRI's proactive stance in enhancing its law enforcement capabilities.

Enhanced Organizational Capacity and Policy Formulation

POLRI has focused on building its technical and operational capacity through specialized training for its personnel in information technology and cybersecurity. Despite these efforts, challenges remain, including a shortage of skilled IT professionals and inadequate sophisticated tools to effectively counter cyberattacks. The formulation of policies responsive to the dynamics of digital crime is essential for ensuring operational effectiveness. These policies must be agile and adaptable to keep pace with the rapid evolution of cyber threats. Additionally, POLRI's efforts to strengthen its legislative framework support the development of comprehensive strategies for combating digital crime.

Collaboration and International Cooperation

Collaboration is a cornerstone of POLRI's strategy to combat cybercrime. The agency has forged strategic partnerships with technology firms, international organizations, and other governmental agencies. These partnerships are vital for leveraging resources, expertise, and information, which are critical in addressing the multifaceted nature of cybercrime. On an international level, POLRI has engaged in various regional and global forums and collaborations, such as the ASEAN Cybersecurity Cooperation Strategy and the Interpol Global Complex for Innovation. These collaborative efforts facilitate the exchange of information, technology, and strategies necessary for tackling transnational cybercrime.

Addressing Cybercrime Trends and Challenges

The increase in cybercrime incidents in Indonesia, with more than 1.2 million cyberattacks recorded in 2023, underscores the urgency of POLRI's strategic transformation. Cybercrimes such as ransomware, phishing, and Distributed Denial of Service (DDoS) attacks are becoming more sophisticated,

necessitating specialized handling and appropriate strategies. The Cyber Crime Directorate, Bareskrim, has taken initial steps to enhance technical and operational capacity, but there is a continuous need for improvement in human resources and technological tools. Furthermore, public digital literacy is crucial for reducing vulnerabilities to cybercrime, highlighting the need for comprehensive educational initiatives.

Comprehensive Analysis and Global Insights

Through a normative juridical legal research method, this paper systematically analyzes the strategic transformation of POLRI, providing a detailed examination of the specific tools, training, and partnerships utilized to tackle digital crime. The study also explores the legislative framework and policies implemented to support this transformation. By integrating various theoretical perspectives, such as technological determinism, routine activity theory, institutional theory, the Public-Private Partnership (PPP) framework, and cybercrime and cybersecurity theory, the paper offers valuable insights into the successes and challenges faced by POLRI. These insights are not only relevant to Indonesia but also provide lessons for law enforcement agencies globally, emphasizing the importance of adaptive strategies, technological advancements, and collaborative efforts in the digital era.

Digital Society Literacy

The digital literacy level of Indonesian society influences the effectiveness of handling cybercrime. Educational programs and awareness campaigns have been implemented, but their scope remains to be debated. Low digital literacy makes many people vulnerable to various types of online fraud and cyberattacks. The National Police needs to collaborate more intensively with educational institutions, non-governmental organizations and the private sector to strengthen efforts to increase digital literacy. Education about cyber security should be included in formal and informal education curricula, and disseminated through social media and public campaigns.

DISCUSSION

The strategic transformation of the Indonesian National Police (POLRI) in response to digital crime highlights several critical areas of focus and development. This discussion examines the effectiveness of these strategies, the challenges encountered, and the broader implications for law enforcement in the digital era.

Effectiveness of Strategic Transformation

POLRI's proactive measures, including organizational restructuring, capacity building, and the adoption of advanced technologies, have been pivotal in enhancing its ability to combat cybercrime. The establishment of specialized units, such as the Cyber Crime Directorate within Bareskrim, underscores the importance of targeted approaches to handle the complexities of cyber threats. The focus on technical training and capacity building has equipped personnel

with the necessary skills to address sophisticated cybercrimes, thereby enhancing operational effectiveness. Moreover, the integration of advanced technological tools for detection and prevention has bolstered POLRI's capacity to respond to cyber incidents swiftly and effectively.

Challenges and Limitations

Despite these advancements, POLRI faces significant challenges that impede its effectiveness. One major issue is the shortage of skilled IT professionals within the police force. The rapid pace of technological change demands continuous upskilling and recruitment of specialized personnel, which remains a persistent challenge. Additionally, the lack of sophisticated tools and systems to detect and counteract cyberattacks limits POLRI's ability to respond proactively. This gap underscores the need for sustained investment in technological infrastructure and human resource development. Another critical challenge is the low level of digital literacy among the general public. Increasing public awareness and knowledge about cyber risks is essential to reduce vulnerabilities and enhance community resilience against cyber threats. Educational initiatives and public awareness campaigns are crucial in this regard, yet they require substantial resources and coordinated efforts across various sectors.

Collaborative Efforts and International Cooperation

POLRI's emphasis on collaboration, both domestically and internationally, has been a cornerstone of its strategy to combat cybercrime. By partnering with technology firms, international organizations, and other governmental agencies, POLRI has leveraged external expertise and resources to enhance its capabilities. International cooperation, as seen through engagements with the ASEAN Cybersecurity Cooperation Strategy and the Interpol Global Complex for Innovation, facilitates the exchange of vital information, technology, and strategies. These partnerships are crucial for addressing the transnational nature of cybercrime and ensuring a cohesive and comprehensive response. However, the implementation and synchronization of policies at national and international levels require further improvement. Discrepancies in legal frameworks and enforcement practices can hinder effective cooperation and the seamless execution of joint operations. Therefore, ongoing efforts to harmonize policies and enhance the integration of collaborative initiatives are necessary to maximize the impact of these partnerships.

Broader Implications for Law Enforcement

The strategic transformation of POLRI provides valuable insights for law enforcement agencies globally. The necessity of continuous adaptation to technological advancements, the importance of building specialized capacities, and the critical role of collaborative efforts are key takeaways. Law enforcement agencies must prioritize technological innovation and foster partnerships with various stakeholders to stay ahead of cybercriminals who exploit digital advancements. Moreover, the need for comprehensive policies that are

responsive to the dynamic nature of cybercrime is evident. Agencies must develop flexible legal frameworks that can quickly adapt to new threats and trends. Public education and awareness are also vital components of a holistic approach to cybersecurity, emphasizing the role of the community in enhancing overall security.

CONCLUSIONS AND RECOMMENDATIONS

The strategic transformation of the Indonesian National Police (POLRI) in dealing with crime in the digital era is an important step that must continue to be optimized to face the increasingly complex threat of cybercrime. This research identifies various aspects that need to be strengthened, including policies and strategies, technology implementation, human resource capacity, international cooperation, and community digital literacy.

The effectiveness of the National Police's policies and strategies in dealing with cybercrime shows progress, but there are still challenges in terms of coordination between institutions and consistency of law enforcement. The adoption of advanced technology has helped the National Police become more proactive in detecting and preventing cybercrime, but infrastructure and budget limitations remain major obstacles. The capacity of Polri's human resources in the field of information technology still requires improvement, especially in terms of technical and operational expertise. Advanced training and certification are an urgent need to address this gap. The high level of personnel rotation also affects the continuity of expertise within the National Police team.

International cooperation carried out by the National Police shows great potential in dealing with cross-border cybercrime, but obstacles such as differences in jurisdiction and limitations in data sharing need to be overcome through more efficient mechanisms. The digital literacy of Indonesian society is still low, which makes many individuals vulnerable to cyberattacks and online fraud. Therefore, educational programs and awareness campaigns must be expanded and deepened.

Recommendations resulting from this research include strengthening policies and coordination between institutions, investing in advanced technology, increasing human resource capacity, increasing international cooperation, and increasing public education and digital literacy. By implementing these recommendations, it is hoped that the National Police can increase effectiveness and efficiency in dealing with crime in the digital era, as well as ensuring the security and order of Indonesian society.

Overall, the National Police's strategic transformation in dealing with crime in the digital era is a journey that requires continuous support from all stakeholders, both at the national and international levels. This effort is not only important to face the threat of cybercrime, but also to build public trust in the National Police's ability to maintain security in an increasingly digital era.

FURTHER STUDY

Future research should delve deeper into the specific impacts of POLRI's strategic transformation on its operational effectiveness in combating cybercrime. Comparative studies between POLRI and other national police

forces that have undergone similar transformations could provide valuable benchmarks and best practices. Additionally, investigating the long-term sustainability of these strategic initiatives, particularly in terms of technological adoption and human resource development, is crucial. Evaluating the effectiveness of educational initiatives aimed at increasing public digital literacy would also be beneficial, as this could highlight gaps and areas for improvement. Moreover, exploring the dynamics of international cooperation, especially the challenges related to jurisdictional differences and data sharing, could lead to the development of more efficient collaborative frameworks. Overall, a multidimensional approach to studying POLRI's strategies, incorporating technological, educational, and international perspectives, will offer comprehensive insights into the ongoing evolution of cybercrime prevention and law enforcement.

ACKNOWLEDGMENT

Thank you for your prayers and support, Sespimma Sespim.Lemdiklat POLRI Batch 71 colleagues who always provide support to me so that I am able to carry out the education process well.

REFERENCES

Akbar, D. L. (2019). Criminal Law Policy in Handling Digital Asset-Based Money Laundering in Indonesia. *Journal of Law and Legal Reform*, *1*(1), 129–176. https://doi.org/10.15294/jllr.v1i1.35543

Ali, Z. (2021). *Metode Penelitian Hukum*. Sinar Grafika.

Arif, M. (2021). Tugas Dan Fungsi Kepolisian Dalam Perannya Sebagai Penegak Hukum Menurut Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian. *Al-Adl : Jurnal Hukum*, *13*(1), 91–101. https://doi.org/10.31602/al-adl.v13i1.4165

Efendi, J., & Rijadi, P. (2022). *Metodologi Penelitian Hukum Normatif dan Empiris* (Kedua). Kencana.

Hermawati, N., & Santiago, F. (2023). Law Enforcement Against Cybercrime in Online Activities. *Edunity : Kajian Ilmu Sosial Dan Pendidikan*, *2*(1), 38–46. https://doi.org/10.57096/edunity.v1i05.34

Irfan, M., Ramdhani, M. A., Darmalaksana, W., Wahana, A., & Utomo, R. G. (2018). Analyzes of cybercrime expansion in Indonesia and preventive actions. *IOP Conference Series: Materials Science and Engineering*, *434*(1). https://doi.org/10.1088/1757-899X/434/1/012257

Lubis, F. (2022). Cyber Crime E-Commerce Business Transactions. *Sasi*, *28*(4), 589. https://doi.org/10.47268/sasi.v28i4.1068

Monique, C., Anggraeny, I., Wardoyo, Y. P., & Slamet, A. B. (2022). The Urgency of Establishing Guidelines for Handling Cybercrime Cases in the Indonesian

National Police Department. *KnE Social Sciences*, *2022*, 349–359. https://doi.org/10.18502/kss.v7i15.12107

Nur, M. S., Puluhuwa, F., & Wantu, F. M. (2022). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Ilmu Hukum "THE JURIS,"* *2*(01), 58–77. https://doi.org/10.61084/jsl.v2i01.7

Nuth, M. S. (2008). Taking advantage of new technologies: For and against crime. *Computer Law and Security Report*, *24*(5), 437–446. https://doi.org/10.1016/j.clsr.2008.07.003

Purwanti, A. (2020). *Metode Penelitian Hukum Teori dan Praktik*. CV Jakad Media Publishing.

Ramli, T. S., Ramli, A. M., Permata, R. R., Ramadayanti, E., & Fauzi, R. (2020). Aspek Hukum Platform e-Commerce dalam Era Transformasi Digtal. *Jurnal Studi Komunikasi Dan Media*, *24*(2), 119. https://doi.org/10.31445/jskm.2020.3295

Sani, A., Sumartias, S., Hafiar, H., & Ismail, N. (2022). West Java Regional Police Public Relations Personnel's adaptation to digital age communication. *PRofesi Humas Jurnal Ilmiah Ilmu Hubungan Masyarakat*, *7*(1), 73. https://doi.org/10.24198/prh.v7i1.38645

Sitorus, R. M., & Amal, B. K. (2022). Police Professionalism in Prevention of Violent Criminal Acts by the Police in Indonesia. *Randwick International of Social Science Journal*, *3*(1), 102–115. https://doi.org/10.47175/rissj.v3i1.380

Wahyudi, S. T., Hadi, S., & Ibrahim, A. L. (2020). Law in The Era of Digitalization and Covid-19 Pandemic. *Veteran Law Review*, *5*(1), 74–88.

Wijaya, M. R., & Arifin, R. (2020). Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime? *IJCLS (Indonesian Journal of Criminal Law Studies)*, *5*(1), 63–74. https://doi.org/10.15294/ijcls.v5i1.23273