Proceedings of Police Academy, Vol.1, No.1, 2025, pp. 119-131

Cybercrime as a Threat to National Security: A Review of the Role and Preparedness of the Indonesian Police

Brandon Romano Abast[1], Daniel Christian Damanik[2], Ghifari Jaya Fahmi[3], Jason Moreno Nanggala Hutagalung[4], Mario Tao Parsaulian Siahaan[5*]

Indonesian Police Academy

Corresponding Email: mariotpsiahaan@gmail.com

Abstract

The rapid advancement of digital technology has significantly altered the landscape of national security in Indonesia, with cybercrime emerging as a critical and complex threat. This study critically examines the role and preparedness of the Indonesian National Police (INP) in addressing cybercrime in the face of increasing digital vulnerabilities. Using a scoping review and thematic synthesis methodology, this research analyzes secondary data from scholarly publications, policy documents, and institutional reports to assess legal, institutional, and operational frameworks. Findings reveal that while the Indonesian government has established foundational measures, substantial challenges persist. These include a shortage of skilled personnel, low public digital literacy, fragmented inter-agency coordination, and outdated legal frameworks. To enhance national cyber resilience, this study recommends the strengthening of human capital through specialized training, improving inter-agency coordination protocols, updating legal instruments to match technological developments, expanding digital literacy campaigns, and fostering international cooperation. Ultimately, addressing cybercrime as a national security threat requires a cohesive, adaptive, and multi-sectoral policy approach. The findings aim to support future strategies to increase Indonesia's capacity to prevent, respond to, and mitigate cyber threats effectively.

Keywords: *Cybercrime, National Security, Indonesian National Police, Cybersecurity Policy, Cyber Threats.*

INTRODUCTION

Study Surroundings

Cybercrime in the Era of Rapid Technological Growth

The rapid advancement of digital technology has significantly transformed various aspects of society, including communication, commerce, and governance. However, this technological progress has also led to a substantial increase in cybercrime incidents, posing serious threats to national security and public trust.

According to Widiasari and Thalib (2022), the proliferation of information technology has facilitated the emergence of diverse cybercrimes in Indonesia, such as data breaches,

identity theft, and unauthorized access to confidential information. Their study emphasizes that the misuse of technology not only infringes on individual privacy but also undermines the integrity of digital infrastructures.

In response to these challenges, the Indonesian government has undertaken legislative measures, including the enactment of Law Number 11 of 2008 on Electronic Information and Transactions, amended by Law Number 19 of 2016. Despite these efforts, studies indicate that the implementation of such laws faces obstacles due to limited resources, lack of specialized personnel, and the evolving nature of cyber threats. To effectively combat cybercrime in this era of rapid technological growth, it is imperative for Indonesia to enhance its cybersecurity infrastructure, invest in capacity building for law enforcement agencies, and foster international collaboration. Such comprehensive strategies are essential to safeguard national security and maintain public confidence in digital systems.

Regional Lessons from Southeast Asia

Cybercrime is a criminal act carried out through computer networks and the usage of the internet. This type of crime is generally conducted online through certain applications or networks that are illegal. According to data from the National Criminal Information Center of the Indonesian Police's Criminal Investigation Agency (Bareskrim Polri), the police handled 8,831 cases of cybercrime from January 1 to December 22, 2022. This number represents a fourteen fold increase compared to the year 2021 (Pusiknas, 2023). This significant rise may indicate that the Indonesian National Police need to develop new strategies to reduce the number of cybercrime cases in Indonesia.

The increase in cybercrime goes hand in hand with the development of technology and information in Indonesia. With such rapid advancements in technology and information, there is also a need to enhance data protection and security on social media or other platforms, which can be the starting point for cybercrime. As stated in The Constitution of the Republic of

Indonesia of 1945, article 30, paragraph 4, “the Indonesian National Police, as a state apparatus responsible for maintaining security and public order, has the duty to protect, nurture, serve the community, and enforce the law.” Therefore, the role of the Indonesian National Police is really crucial in taking firm action against all perpetrators of cybercrime. In light of the aforementioned issues, this essay is composed with the objective of critically examining the role and preparedness of the Indonesian National Police in addressing and managing cybercrime cases within Indonesia.

Aim of Study

This study aims to provide a comprehensive and critical review of the role and preparedness of the Indonesian National Police in addressing cybercrime, which has emerged as a significant threat to national security. It seeks to examine the current strategies and policies implemented by the police force to combat cybercrime, assess their technological capabilities and human resource readiness, and identify the key challenges faced in preventing and managing such crimes. Furthermore, this study can serve as a reference for developing new strategies to enhance the effectiveness and capacity of the Indonesian National Police in safeguarding the nation against the evolving landscape of cyber threats.

METHOD

Methodology

Data Collection Technique

The data collection techniques employed in this study is secondary data analysis, whereby data are gathered from previously published and established sources. The references utilized in this research include scholarly journals, news publications, articles, and other credible literature that explore the issue of cybercrime, technological advancement, and the role of the Indonesian National Police in addressing various forms of cyber-related offenses.

Data Analysis Technique

This study employs a scoping review methodology, originally proposed by Arksey and O'Malley (2005), complemented by thematic synthesis for data analysis, a method developed by Thomas and Harden (2008). The scoping review facilitates the systematic identification and selection of relevant literature concerning cybercrime, national security, and the role of the Indonesian National Police. Subsequently, thematic synthesis is applied to analyze and categorize key findings from the selected sources into major themes, including police preparedness, technological advancement, and policy challenges. The findings are then organized into a structured overview of the role and preparedness of the Indonesian National Police in managing cybercrime.

Literature Review

Cybercrime

Cybercrime refers to unlawful activities conducted using digital technologies, often targeting computer systems, data networks, or internet-based platforms. These crimes encompass a wide range of offenses, including identity theft, cyber fraud, phishing, ransomware, unauthorized access, and the spread of malicious software. The proliferation of internet access and digital technologies has significantly transformed the nature of crime, shifting from physical to virtual environments where detection and prosecution are more complex (Kshetri, 2019).

In Indonesia, the expansion of internet connectivity has led to a parallel surge in cybercrime cases. Indonesia has experienced a steady rise in digital offenses, especially those involving online scams, financial fraud, and attacks on government systems (Simanjuntak, 2022). Moreover, cybercriminals in Indonesia often exploit gaps in digital literacy, weak cybersecurity protocols, and limited law enforcement capacity. These vulnerabilities enable not only local cybercriminal groups to operate with relative ease but also open pathways for

transnational cybercrime syndicates to target Indonesian institutions and individuals (Wijayanto & Sihombing, 2020). The dynamic and often borderless nature of cybercrime therefore demands a multifaceted response, involving legal, technical, institutional, and educational measures to ensure effective prevention and control.

National Security

National security is fundamentally concerned with safeguarding a state's sovereignty, territorial integrity, and the welfare of its citizens from threats that can arise both externally and internally. Traditionally, this concept focused mainly on military defense against external aggression. However, contemporary understandings of national security have broadened to include non-military challenges such as terrorism, economic instability, environmental issues, pandemics, and increasingly, cyber threats (Buzan, Wæver, & de Wilde, 1998).

National security encompasses not only protection from military threats but also the maintenance of social order and resilience against various disruptions, including political instability and economic crises. This broader perspective acknowledges the interconnected nature of global risks in an era marked by globalization and technological advancement. In the modern context, threats such as cybercrime have become critical concerns that must be addressed, as they can undermine national security in unconventional ways, including attacks on critical infrastructure, theft of sensitive data, and disruption of social stability through information manipulation (Baldwin, 1997).

RESULTS AND DISCUSSION

The Indonesian government has acknowledged cybercrime as a critical threat to national security and has taken several steps to mitigate its impact. One significant measure is the formation of specialized units within the Indonesian National Police, such as the Cyber Crime Directorate, which focuses exclusively on handling cyber-related offenses. In addition to

institutional efforts, Indonesia has enacted Law No. 19 of 2016 on Electronic Information and Transactions (ITE Law), providing a legal framework to address various cybercrimes including hacking, online fraud, and the spread of illegal content. The government has also established the National Cyber and Crypto Agency (BSSN) to coordinate cybersecurity policies, enhance the protection of critical infrastructure, and respond to cyber incidents effectively. Collaborative efforts involving governmental bodies, private sectors, and international organizations have further supported Indonesia's efforts to build resilience against cyber threats.

Despite these initiatives, challenges persist that hinder the full effectiveness of cybercrime mitigation. A major issue lies in the shortage of skilled personnel proficient in cyber forensics and digital investigations, which limits the capacity of law enforcement agencies to keep up with the fast-evolving techniques used by cybercriminals. Furthermore, bureaucratic complexities and unclear jurisdictional boundaries among different agencies often delay prompt action, weakening the overall response to cyber threats. Public awareness regarding cybersecurity remains low, particularly in remote regions where digital literacy is uneven, increasing vulnerability to attacks such as phishing and ransomware. The country's large and diverse population adds complexity to the task of fostering widespread cybersecurity awareness.

To improve Indonesia's preparedness in facing cybercrime, enhancing human resource development through specialized training and certification programs is crucial. Strengthening coordination mechanisms across agencies with clear protocols and improved communication channels will enable faster and more cohesive responses to cyber incidents. Moreover, expanding public education campaigns aimed at increasing cybersecurity awareness can empower individuals and organizations to better protect themselves. Updating and harmonizing legal regulations to reflect the rapid advancements in technology and emerging cyber threats will also strengthen the legal basis for enforcement. Finally, given the transnational nature of

cybercrime, fostering greater international collaboration by participating in global cybercrime prevention initiatives and sharing best practices will significantly enhance Indonesia's defensive capabilities. Here is a table that explains the shortcomings of each thing made to address and manage all cybercrime cases and the specific issues associated with them.

Table 1: Cybercrime Aspects and Specific Issues Associated

Aspect	**Government Measures**	**Shortcomings**	**Recommendations**
Legal Framework	ITE Law No.19/2016	Law enforcement capacity limited	Update laws regularly, improve enforcement
Institutional Capacity	Cyber Crime Directorate, BSSN	Limited trained personnel	Increase training, certification programs
Public Awareness	Awareness campaigns	Low digital literacy in many regions	Expand education and outreach
Interagency Coordination	Policy frameworks for cooperation	Bureaucratic delays, unclear roles	Establish clear protocols, improve communication
International Cooperation	Partnerships with global law enforcement agencies	Limited engagement	Enhance participation in global forums

Despite the Indonesian government's implementation of key regulatory and institutional measures, such as the enactment of Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE Law), the establishment of the Cyber Crime Directorate within the Indonesian National Police, and the formation of the National Cyber and Crypto Agency (BSSN), cybercrime incidents in the country continue to increase in frequency and complexity.

According to BSSN's 2022 annual report, Indonesia recorded over 1.4 billion attempted cyberattacks throughout the year, underscoring the critical scale of digital threats faced by the nation. While these efforts mark a significant step toward institutionalizing cybersecurity governance, their effectiveness remains limited due to several persistent challenges.

The enforcement of the ITE Law, for instance, is hindered by regulatory ambiguities and inconsistent implementation, reducing its deterrent power. Moreover, both BSSN and the Indonesian National Police continue to face shortages in specialized human resources, particularly in the areas of cyber forensics and digital investigation. Another critical gap is the lack of adequate digital literacy among the general population, especially in rural and remote regions, which exacerbates vulnerability to cybercrimes such as phishing, online scams, and misinformation. These ongoing limitations indicate that while foundational structures are in place, further advancements in legal clarity, personnel capacity building, inter-agency coordination, and public cybersecurity awareness are necessary to strengthen Indonesia's overall cyber resilience.

So, to enhance Indonesia's capacity in mitigating cybercrime and strengthening national cybersecurity, several strategic recommendations must be considered:

- First, it is essential to invest in the development of human capital through targeted training and certification programs for law enforcement personnel, digital forensic analysts, and cybersecurity professionals. This will ensure the availability of skilled experts capable of addressing increasingly sophisticated cyber threats.

- Second, inter-agency coordination should be improved through the establishment of standardized operating procedures and integrated information systems that enable real-time collaboration between relevant institutions such as BSSN, the Indonesian National Police, and the Ministry of Communication and Information Technology.

- Third, the government must revise and update existing cybersecurity legislation to address regulatory gaps, particularly those related to emerging technologies like artificial intelligence, deep fakes, and blockchain-based crimes.

- Fourth, public awareness campaigns should be scaled up using both traditional and digital media to promote digital literacy and encourage secure online behavior across all demographics, particularly in rural areas. Lastly, Indonesia should deepen its engagement in international cybersecurity cooperation frameworks and expand bilateral or multilateral partnerships for information exchange, joint operations, and capacity building, recognizing the transnational nature of cybercrime.

CONCLUSION

Conclusion

In an era characterized by rapid technological advancement, cybercrime has emerged as a significant threat to national security in Indonesia. The increasing frequency and complexity of cyber offenses underscore the urgency for a robust and adaptive national cybersecurity strategy. This study has examined the role and preparedness of the Indonesian National Police in addressing cybercrime, revealing both substantial progress and persistent gaps. Institutional developments such as the establishment of the Cyber Crime Directorate and the National Cyber and Crypto Agency (BSSN), as well as the enactment of the ITE Law, demonstrate the Indonesian government's commitment to enhancing cybersecurity governance. However, challenges such as limited human resource capacity, inadequate digital literacy, bureaucratic inefficiencies, and fragmented legal implementation continue to hinder the effectiveness of these initiatives.

The findings of this study highlight the necessity of a multifaceted approach to cybercrime prevention and response. Strengthening human capital through specialized training,

fostering inter-agency coordination through clear protocols and integrated systems, updating cyber legislation to reflect technological developments, and expanding public awareness campaigns are crucial steps toward building national cyber resilience. Moreover, increased participation in international cybersecurity collaboration will equip Indonesia with the tools and knowledge necessary to combat transnational cyber threats more effectively. In conclusion, while the foundational structures for combating cybercrime have been established, continuous investment, strategic refinement, and adaptive governance are essential to securing Indonesia's digital future and protecting its national interests in the cyber domain.

Policy Implications

The findings of this study reveal significant policy implications for strengthening Indonesia’s national capacity to combat cybercrime as a threat to national security. First and foremost, there is an urgent need for the Indonesian government to adopt a comprehensive national cybersecurity strategy that aligns legal, institutional, and operational frameworks under a unified policy vision. This strategy must be proactive, adaptive, and integrated across all levels of government, emphasizing prevention, deterrence, and resilience.

From a regulatory perspective, the current legislative framework (particularly the ITE Law) must be periodically reviewed and revised to keep pace with the rapid evolution of cyber threats and emerging technologies. This includes the development of specific legal instruments to address crimes involving artificial intelligence, digital currencies, deepfake technologies, and other advanced cyber tools. Such revisions should also aim to reduce ambiguity, ensure proportionality in enforcement, and uphold human rights principles, particularly concerning freedom of expression and privacy.

In terms of institutional capacity, policy must prioritize investment in specialized human resources. This entails allocating adequate funding for continuous education, advanced training, and internationally recognized certification programs for law enforcement personnel,

prosecutors, and judicial actors involved in cybercrime investigation and prosecution. Establishing cybercrime units in regional police offices across Indonesia can decentralize capacity and improve response times, particularly in underserved areas.

Effective interagency coordination is another critical area for policy intervention. The government should institutionalize clear standard operating procedures (SOPs) and develop interoperable digital platforms for real-time information exchange among key stakeholders such as BSSN, the Indonesian National Police, the Ministry of Communication and Information Technology, and the judiciary. A national cyber incident response protocol should be adopted to ensure cohesive and timely action in the face of cyberattacks.

From a public engagement standpoint, policy efforts must include long-term digital literacy and cybersecurity awareness programs, embedded within the national education curriculum and community outreach initiatives. Increasing public knowledge of digital risks and best practices will not only reduce victimization rates but also foster a culture of shared responsibility in safeguarding the digital space.

In summary, the development of a coherent, forward-looking, and multi-sectoral cybersecurity policy framework is essential to address the growing cybercrime challenge. The adoption of such policies will not only enhance Indonesia’s national security but also foster trust in digital systems, which is critical for economic growth and democratic resilience in the information age.

REFERENCES

Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. International Journal of Social Research Methodology, 8(1), 19–32. https://doi.org/10.1080/1364557032000119616

Badan Siber dan Sandi Negara (BSSN). (2022). Laporan Tahunan BSSN 2022. https://bssn.go.id

Badan Siber dan Sandi Negara (BSSN). (2023). Annual Report on National Cybersecurity. Jakarta: BSSN Publications.

Baldwin, D. A. (1997). The concept of security. Review of International Studies, 23(1), 5–26.

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.

Djarawula, M., et al. (2024). The impact of digital technology developments on criminal law in Indonesia. International Journal of Multidisciplinary Research and Growth Evaluation, 5(6), 1014–1019.

Eastasouth Institute. (2023). Cybercrime law enforcement challenges in Indonesia. Journal of Social and Human Sciences. https://sj.eastasouth-institute.com

Hypernet. (2022). Kasus cybercrime di Indonesia kian mengkhawatirkan. https://www.hypernet.co.id

Interpol. (2023). International cooperation on cybercrime. Retrieved from https://www.interpol.int/en/Crimes/Cybercrime

Kshetri, N. (2019). Cybercrime and cybersecurity in the global South. Palgrave Macmillan.

Kominfo. (2022). Indonesia's cybersecurity framework and policies. Ministry of Communication and Information Technology.

Kopusindo Journal. (2023). Literasi digital dan keamanan siber di wilayah perdesaan Indonesia. https://jurnal.kopusindo.com

Pratama, H., & Suhendra, I. (2021). Enhancing digital forensics capacity in Indonesian law enforcement: Challenges and recommendations. Journal of Cybersecurity Research, 5(2), 85–98.

Pusiknas Polri. (2023). Kejahatan siber di Indonesia naik berkali-kali lipat. https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

Santosa, M. (2019). Legal framework and enforcement of cybercrime in Indonesia: Analysis of the ITE Law. Indonesian Journal of Law and Policy, 7(1), 45–60.

Simanjuntak, R. (2022). Cybercrime trends in Indonesia: A five-year review. Jurnal Kriminologi Indonesia, 13(1), 55–68.

Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. BMC Medical Research Methodology, 8(1), 45. https://doi.org/10.1186/1471-2288-8-45

UBHARAJAYA Journal. (2022). Tantangan penegakan hukum kejahatan siber di Indonesia. https://ejurnal.ubharajaya.ac.id

Widiasari, N. K. N., & Thalib, E. F. (2022). The impact of information technology development on cybercrime rate in Indonesia. Journal of Digital Law and Policy, 1(2), 73–86.

Wahyudi, A., Setiawan, R., & Haryanto, A. (2020). Digital literacy and cybersecurity awareness in Indonesia's diverse population. Journal of Information Security, 11(3), 120–132.

Wijayanto, A., & Sihombing, D. (2020). Institutional challenges in cybercrime enforcement in Indonesia. Indonesian Journal of Policing Studies, 4(2), 112–127.