Journal of Mathematics Instruction, Social Research and Opinion
Vol. 5, No. 1, March 2026, pp. 991 – 1005, https://doi.org/10.58421/misro.v5i1.1315
ISSN 2962-7842

Cybercrime Growth and Law Enforcement Challenges in Indonesia: A Cybercriminology Perspective

Kuswardani[1], Marisa Kurnianingsih[2], Andria Luhur Prakosa[3], Fahmi Fairuzzaman[4]
[1,2,3,4]Faculty of Law, Muhammadiyah University of Surakarta, Indonesia

Article Info

Article history:

Received 2026-02-20
Revised 2026-03-30
Accepted 2026-03-31

Keywords:

Criminology
Cyber Criminology
Cyber Law
Cybercrime
Law Enforcement

ABSTRACT

This study examines the increasing complexity of cybercrime in Indonesia, which is influenced not only by technological development but also by the interaction of individual, structural, and institutional factors in digital environments. The objective is to analyze criminological factors contributing to cybercrime and to examine law enforcement challenges from a cybercriminology perspective in Indonesia. This research uses a normative juridical method with a qualitative approach based on secondary data obtained from legal documents, scientific literature, and previous studies. Data were collected through a systematic literature review and document analysis. The findings show that cybercrime is driven by offender motivation and rationality, technological accessibility, anonymity, and opportunity structures in cyberspace. Law enforcement faces challenges such as difficulties in identifying perpetrators, limited digital forensic capacity, regulatory gaps, and jurisdictional constraints due to the transnational nature of cybercrime. This study contributes to cybercriminology by integrating criminological and legal perspectives into a unified analytical framework for understanding cybercrime as a multidimensional phenomenon. The implication is that effective cybercrime countermeasures require strengthening legal frameworks, institutional capacity, and technological readiness.

Corresponding Author:

Kuswardani
Faculty of Law, Muhammadiyah University of Surakarta, Indonesia
Email: kus283@ums.ac.id

1. INTRODUCTION

The increasing trend of cybercrime in Indonesia in recent years is reflected in the growing number of reported cases, including online fraud, personal data breaches, and malware-based attacks targeting both individuals and institutions. Advancements in information technology do not solely drive this phenomenon, but are also driven by the transformation of social interaction patterns into digital spaces. Compared to conventional crimes, cybercrime demonstrates distinct characteristics, particularly in terms of perpetrator

anonymity and its ability to operate across geographical boundaries. Previous studies indicate that the complexity of cybercrime continues to escalate alongside the rising dependence of society on digital technology and internet usage [1]. This condition places internet users, especially students, in a highly active digital group, in a vulnerable position to various forms of cyber exploitation.

The impact of cybercrime extends beyond financial losses to include psychological and social consequences that affect victims over time. Individuals who experience online fraud or personal data breaches often report a diminished sense of security in digital environments, accompanied by heightened concerns regarding the misuse of their personal information. Among specific social groups such as students, high levels of digital engagement are associated with increased exposure to cybercrime risks. Empirical studies indicate that limited digital security literacy significantly contributes to individual vulnerability to various forms of technology-based crimes, including social engineering and data exploitation [2]. This condition suggests that the effects of cybercrime are not merely incidental but also influence behavioral patterns and risk perceptions in the use of digital technologies.

The rapid advancement of information technology in Indonesia has accelerated the transformation of social, economic, and communication activities into an increasingly integrated digital environment. The expansion of internet users and the widespread adoption of digital platforms have enhanced opportunities for interaction, while simultaneously creating new avenues for technology-based crimes. The borderless nature of cyberspace enables interactions without physical contact, thereby weakening conventional mechanisms of social control. In this context, cybercrime emerges as a consequence of digital social dynamics that are not fully supported by the readiness of adaptive security systems and regulatory frameworks [3]. This condition indicates that digital transformation not only improves efficiency but also generates structural vulnerabilities within technology-driven social systems.

The transformation of crime patterns from conventional to digital-based forms has become a central concern in contemporary criminological studies. Criminal activities that once depended on physical interaction are increasingly mediated by technology, enabling offenders to operate without direct presence at the crime scene. In this context, a cybercriminology approach is employed to analyze these dynamics by emphasizing the interaction between offenders, technological systems, and the digital environment as the locus of criminal activity. Existing studies highlight that cybercrime is characterized by anonymity, spatial flexibility, and the capacity of offenders to adapt to evolving security mechanisms [4]. This perspective provides a relevant analytical framework for understanding how criminal behavior evolves within complex digital ecosystems.

Recent developments in cybercrime indicate an increasing complexity of modus operandi, particularly in the exploitation of advanced technologies to avoid detection. The use of tools such as Virtual Private Networks (VPNs), encryption methods, and anonymous digital platforms enables offenders to effectively conceal their identities and geographic locations. In addition, the transnational nature of cybercrime creates jurisdictional challenges that complicate law enforcement processes, especially when perpetrators and victims are

located in different countries. Previous studies highlight that these conditions hinder investigation procedures and the collection of legal evidence due to limited access and weak international coordination [5]. This reflects that technological advancement not only enhances the efficiency of digital activities but also broadens the scope for more sophisticated cybercrime practices.

Various challenges in cybercrime law enforcement in Indonesia indicate a structural gap between rapid technological development and the institutional capacity of law enforcement agencies. The identification of perpetrators is often constrained by technical limitations, particularly in tracing altered or anonymized digital footprints that are deliberately designed to hinder forensic tracking. In addition, the shortage of human resources with specialized expertise in digital forensics further reduces the effectiveness of investigative processes. From a regulatory perspective, existing legal frameworks have not fully adapted to the fast-evolving nature of cybercrime, resulting in legal ambiguity in several investigative procedures. These constraints collectively affect the quality of evidence collection and weaken inter-agency coordination in handling cybercrime cases [6].

Several studies have examined cybercrime in Indonesia from legal, institutional, and public policy perspectives. Anwary (2022) [7] emphasizes the role of public administration in strengthening cybercrime prevention through regulatory enhancement and inter-agency coordination mechanisms. Imran (2023) [1] highlights law enforcement officers' perceptions of cybercriminology, indicating the need to improve institutional capacity in understanding the evolving characteristics of digital crime. From a legal perspective, Widijowati (2022) [6] identifies significant complexities in cybercrime handling, particularly due to limitations in existing regulatory instruments. In addition, Sunggara and Hariansah (2024) [2] underline the transnational nature of cybercrime, which creates jurisdictional challenges and complicates international law enforcement cooperation.

Despite the growing body of literature on cybercrime in Indonesia, significant limitations remain in the integration of criminological perspectives with comprehensive legal analysis. Existing studies predominantly emphasize normative and institutional dimensions of cybercrime, while paying limited attention to offender behavior in digital environments and the mechanisms underlying cybercriminal actions. This narrow focus results in an incomplete understanding of cybercrime as a dynamic phenomenon shaped by the interaction between technology, opportunity structures, and individual motivations.

Given the complexity of cybercrime, a multidisciplinary approach is required to capture its evolving nature more comprehensively. In particular, the behavioral adaptation of offenders in response to technological advancements remains underexplored in the Indonesian context. Although Butarbutar (2025) [4] notes that regulatory developments have not been accompanied by adequate criminological understanding of offender adaptation in cyberspace, empirical and integrative analyses remain limited. This indicates a clear research gap in developing a cybercriminology-based framework that systematically incorporates behavioral, technological, and legal dimensions in explaining cybercrime phenomena.

This study aims to analyze the increasing phenomenon of cybercrime in Indonesia from a cybercriminology perspective, focusing on the interaction between offenders, technology, and the digital social environment. Specifically, this research investigates the

criminological factors that influence cybercrime patterns and examines the key challenges in cybercrime law enforcement. In addition, it evaluates the responsiveness of the existing legal framework in addressing the evolving dynamics of cybercrime within a digital society. By integrating criminological and legal perspectives, this study seeks to develop a more structured analytical understanding of how technological advancement shapes contemporary crime patterns in Indonesia.

This research is expected to enrich the development of criminology studies, particularly in understanding cybercrime as a social phenomenon integrated with the development of digital technology. From an academic perspective, this research provides an analytical foundation that connects the cybercriminology perspective with the dynamics of law enforcement in Indonesia. From a practical perspective, the results of this study can serve as a reference for law enforcement officials and policymakers in formulating more adaptive strategies to the characteristics of cybercrime, including increasing institutional capacity and strengthening regulations relevant to technological developments. Furthermore, this research also has implications for increasing public awareness of the risks of crime in the digital space.

2. METHOD

This study employs a normative juridical approach, focusing on the analysis of legal norms governing cybercrime in Indonesia. This approach is used to assess the conformity of existing regulatory frameworks with the evolving dynamics of cybercrime in a digital society [8]. The study examines statutory regulations, legal doctrines, and judicial decisions to understand the legal construction underlying cybercrime law enforcement. The normative juridical approach enables a systematic evaluation of legal principles, norms, and provisions that form the basis of cybercrime regulation and enforcement [9].

The data used in this study are secondary data obtained through a structured literature review. The selection of literature and legal sources is based on the following criteria: (1) relevance to cybercrime, cyber law, or cybercriminology; (2) publication in peer-reviewed journals, accredited national journals (SINTA), or indexed international journals; (3) publication within the last ten years to ensure contemporary relevance; and (4) inclusion of primary legal sources such as Indonesian laws and regulations related to cybercrime. Sources that do not meet these criteria were excluded to maintain analytical validity and academic rigor. The primary legal materials include Indonesian legislation related to cybercrime, while secondary materials consist of scholarly journal articles, books, and prior empirical studies [10]. Documentation techniques and systematic academic database searches were used to collect relevant literature on cybercriminology and law enforcement in Indonesia [11].

The data analysis was conducted using a qualitative descriptive-analytical method through a step-by-step process. First, all collected legal and academic sources were organized and categorized based on thematic relevance (e.g., legal framework, criminological perspective, and enforcement challenges). Second, the selected materials were critically read and coded to identify recurring patterns and conceptual relationships. Third, an interpretation was conducted to examine the interaction between criminological factors and legal norms in addressing cybercrime. Finally, a synthesis was performed to

evaluate the effectiveness of existing regulations in responding to the transnational and adaptive nature of cybercrime. This systematic analytical process ensures a structured and transparent examination of the research problem from a cybercriminology perspective [12].

3. RESULTS AND DISCUSSION

3.1. Results

Patterns and Characteristics of Increasing Cyber Crime in Indonesia

The rise in cybercrime in Indonesia is inextricably linked to the accelerated use of digital technology in various social and economic activities. The transformation of interaction patterns from physical to virtual spaces has transformed the structure of social relationships, becoming more open and network-based. This change creates new opportunities for crime that are no longer dependent on geographic proximity. In this context, the expansion of internet access contributes to increased individual exposure to the risks of digital crime, particularly when economic activities and communications are conducted through online platforms [13]. This trend demonstrates that technological development not only generates efficiency but also creates new vulnerabilities in the digital social structure.

The correlation between the increase in the number of internet users and the growth in cybercrime cases indicates a structural relationship within the digital ecosystem. Expanded technological access allows perpetrators to reach victims on a larger scale without clear spatial boundaries. In this environment, opportunities for crime are determined not only by the perpetrator's intentions but also by the availability of means and weak control mechanisms in the digital space [14]. This phenomenon demonstrates that the development of digital infrastructure contributes to the formation of new configurations of crime patterns. An analysis of these dynamics shows that technological expansion serves as a medium accelerating the diffusion of cybercrime in society.

The dominance of economically based crimes in the form of online fraud, phishing, and personal data theft reflects perpetrators' adaptation to people's digital activity patterns. The intense use of e-commerce and digital financial services creates an interactive space rife with the exchange of sensitive information. In this situation, perpetrators exploit system vulnerabilities and user behavior to gain profit [15]. The characteristics of these crimes demonstrate that the success of criminal acts depends not only on technical skills but also on an understanding of the victim's digital interaction patterns. This pattern is consistently identified in research on online fraud in Indonesia, which places information manipulation as a key element.

In addition to economically motivated crimes, there are also forms of cybercrime that involve higher technical capacity and impact broader systems. Activities such as cyberespionage and attacks on digital infrastructure demonstrate a shift toward organized, technology-based crime. The resulting impact is not limited to individual losses but can also impact institutional stability and information security [3]. This variation demonstrates that cybercrime has multiple dimensions, ranging from simple to complex. Analysis of this spectrum demonstrates the importance of understanding the differences in characteristics between types of crime in the context of policy and response.

The characteristics of cybercrime perpetrators demonstrate patterns that do not fully align with conventional criminal typologies. Individuals involved often possess specific technical skills and a sufficient level of digital literacy. This indicates that access to technology is a crucial factor in explaining a person's involvement in cybercrime. Furthermore, the perpetrator's social background is not always the primary indicator, as technical skills can be acquired through various open sources on the internet [16]. This phenomenon emphasizes that analyzing cybercrime perpetrators requires an approach that takes the technological dimension into account more specifically.

The anonymity of digital spaces significantly contributes to the increased opportunities for cybercrime. The ability to disguise identity through various technologies creates conditions that complicate the process of identifying and tracing perpetrators. In this situation, the risk of being caught is relatively different compared to conventional crimes occurring in physical spaces. This factor influences the perpetrator's rational considerations when committing crimes, particularly in the context of calculating risks and benefits. Analysis of the role of anonymity shows that technological structures contribute to shaping criminal behavior in cyberspace [17].

The development of modus operandi in cybercrime demonstrates an adaptive pattern that follows changes in technology and user behavior. Social engineering techniques are used to influence victims' perceptions, while system exploitation is carried out to gain access to data or digital resources. A combination of technical and psychological approaches is a key characteristic of cybercrime practices. In many cases, perpetrators rely not only on software or systems but also exploit weaknesses in victims' decision-making [18]. This dynamic suggests that the success of cybercrime is the result of the interaction between technological and human factors.

Digital platforms, which command a high level of trust in society, are vulnerable to abuse. Marketplaces, social media, and digital financial applications provide an environment of intensive interaction with a relatively high level of user trust. Perpetrators exploit this situation to insert illegal activities into seemingly normal transaction flows. The trust structure within the digital ecosystem is an element that can increase vulnerability to cybercrime [19]. Analysis of this phenomenon shows that digital security depends not only on the system but also on the patterns of social interaction formed within it.

The transnational dimension of cybercrime adds complexity to understanding and addressing this crime. Perpetrators can operate from different regions than victims, creating obstacles in the application of legal jurisdiction. Differences in legal systems and limited international cooperation are factors that impact the effectiveness of law enforcement [20]. This situation demonstrates that cybercrime cannot be analyzed exclusively within a national framework but requires a broader perspective. This complexity demonstrates the interconnectedness of law, technology, and international relations.

The interaction between technological factors, individual behavior, and institutional factors shapes the dynamic development of cybercrime in Indonesia. The existence of gaps in digital systems, combined with the perpetrator's ability to exploit opportunities, creates conditions that support the occurrence of crime [21]. From the criminological perspective of Cohen & Felson in [22], this condition aligns with Routine Activity Theory, which

emphasizes the intersection between motivated perpetrators, vulnerable targets, and weak supervision. Rational Choice Theory explains perpetrators' actions as the result of considering opportunities and risks in the digital environment [23]. Cybercrime reflects the complex interaction between technology and digital social structures.

Analysis of Criminological Factors in Cybercrime

The behavior of perpetrators in cybercrime demonstrates a close link to individual motivational dimensions that cannot be reduced solely to economic incentives. In many cases, these actions are also influenced by the need for recognition, exploration of technical capabilities, and the urge to experiment in the digital environment. The characteristics of cyberspace, which enable interaction without geographical boundaries, provide space for individuals to develop different behavioral patterns compared to offline contexts. These motivations develop along with the intensity of an individual's involvement in digital activities, expanding access to criminal opportunities [24]. This pattern suggests that individual psychological and social dimensions play a role in shaping the orientation of actions in cybercrime.

Rational considerations are a crucial element in explaining the actions of cybercriminals. Rationality in this context relates not only to the calculation of economic gain but also includes an assessment of the risk of detection and legal consequences. In the digital environment, the perception of a low probability of law enforcement influences an individual's decision to engage in illegal activities. Technological structures allow perpetrators to minimize their digital footprint through various techniques, thus reinforcing the belief that such actions are relatively safe [3]. This pattern aligns with the Rational Choice Theory framework, which positions individuals as actors who consider options calculatively in certain situations.

The perpetrator's technical capabilities also influence this dimension of rationality in utilizing digital systems. Individuals with high technological literacy have a greater capacity to identify security gaps and exploit system weaknesses. This ability not only increases the likelihood of crime success but also fosters the perception that the act can be effectively controlled. In this context, rationality does not stand alone but interacts with an individual's technical competence. The relationship between technological knowledge and criminal behavior suggests that cybercrime develops within a different framework than conventional crime, which relies more on physical interaction [25].

Structural factors in cybercrime relate to the availability of access to technology and digital infrastructure. Increasing access to the internet and digital devices creates conditions that allow for increased interaction in cyberspace. This not only expands opportunities for legal activity but also opens up the possibility of deviance. The digital environment provides a variety of platforms that can be exploited to conduct illegal activities with varying levels of complexity. These developments demonstrate that technological structures play a role in shaping the context in which crime occurs, particularly in terms of ease of access and flexibility in using digital systems [26].

Anonymity is one of the key characteristics that distinguishes cybercrime from other forms of crime. The ability to conceal identity in digital spaces creates conditions that

influence individual behavior in interactions. Individuals tend to exhibit different behavioral patterns when their identities cannot be directly verified. This phenomenon is related to changes in social control occurring in cyberspace, where social norms are not always strongly internalized. Anonymity not only functions as a means of identity protection but also as a factor that facilitates deviant behavior by reducing psychological barriers [27].

The characteristics of available targets also influence opportunities for crime in digital spaces. In the context of cybercrime, targets are not always individuals, but can be data, systems, or digital identities. The target vulnerability is related to the level of system security and user behavior in managing personal information. Individuals who lack an adequate understanding of digital security tend to be easier targets for perpetrators [21]. This pattern suggests that opportunities for crime are not solely determined by the perpetrator, but also by the conditions of the target within a particular digital environment.

Interactions between perpetrators and targets in cyberspace do not require physical presence, thus expanding the possibility of crime. This allows perpetrators to reach victims on a wider scale at a relatively low cost [14]. Within the framework of Routine Activity Theory [25], this situation reflects the intersection of motivated perpetrators, suitable targets, and weak oversight. These three elements are present in different forms in digital spaces, primarily due to the limited availability of effective control mechanisms. Analysis of this pattern suggests that the structure of interactions in cyberspace facilitates crime on a more complex scale.

The digital environment also shapes social interaction patterns that contribute to the development of cybercrime. Digital platforms enable the formation of social networks that can be used to share information, including information related to criminal techniques and strategies. In some cases, this interaction results in collaboration between individuals, increasing the perpetrator's capacity to commit illegal acts. The existence of online communities demonstrates that cybercrime is not always individualistic but can develop in a collective context [28]. This dynamic suggests that the social environment in the digital space plays a role in reinforcing criminal behavior patterns.

Institutional factors also influence the dynamics of cybercrime through monitoring and law enforcement capacity. Limited resources and technological complexity present challenges in identifying and prosecuting perpetrators. Furthermore, differences in jurisdictions in cyberspace add complexity to the law enforcement process. This creates opportunities for perpetrators to evade detection. The interplay between structural weaknesses and perpetrator capabilities suggests that institutional factors play a significant role in shaping opportunities for crime in the digital space [29].

The interplay between individual, structural, and digital environmental factors demonstrates that cybercrime is a phenomenon shaped by multidimensional relationships. The perpetrator's motivation and rationality interact with the anonymity and opportunities available in digital systems, while limited oversight increases the likelihood of crime. Within the theoretical framework, the integration of Rational Choice Theory, Routine Activity Theory, and Space Transition Theory explains how individuals adapt their behavior in digital environments, which differ from physical spaces. This pattern reflects the transformation of

social structures that influence crime dynamics and demonstrates that criminological analysis needs to consider the interrelationship between technology and social behavior [24].

Challenges of Law Enforcement against Cybercrime in Indonesia

The development of cybercrime in Indonesia presents significant challenges to the law enforcement system, which was originally designed to address conventional crimes. The transformation of crime into the digital space has created changes in the characteristics of criminal acts, including in terms of proof, perpetrator identification, and evidence collection. The territorially based legal system faces limitations in reaching criminal activities that are not bound by specific geographic boundaries [13]. In this context, the dynamics of cybercrime require adjustments to law enforcement mechanisms to respond to increasingly complex crime patterns.

The process of identifying perpetrators in cybercrime often faces technical obstacles related to the use of technology to conceal identities. Perpetrators can utilize various tools, such as virtual private networks and encryption, to obscure the digital traces they leave behind. This situation impacts the effectiveness of investigations because it requires higher technical skills than conventional crimes [30]. This complexity indicates that the success of law enforcement depends not only on legal procedures but also on the technological capacity of law enforcement officials.

Limited human resources are one factor affecting the effectiveness of handling cybercrime cases. Law enforcement in this area requires specialized expertise in digital forensics, data analysis, and an understanding of information technology systems. Not all law enforcement officers possess these competencies, which can hinder the investigation process in interpreting digital evidence [31]. The gap between competency requirements and available capacity highlights challenges in developing human resources relevant to technological developments.

Regulatory aspects are also a factor influencing law enforcement against cybercrime in Indonesia. Existing laws and regulations often face limitations in accommodating new and evolving forms of crime. Rapid technological change is not always accompanied by commensurate regulatory updates, resulting in a mismatch between legal norms and criminal practices on the ground [32]. Analysis of the legal framework indicates the need for regulatory adjustments to be more responsive to the dynamics of cybercrime.

Jurisdictional issues pose another challenge in law enforcement against cybercrime, particularly in cases involving perpetrators and victims from different countries. The cross-border nature of cybercrime presents difficulties in determining applicable legal authority. Furthermore, differences in legal systems between countries and limited international cooperation mechanisms slow down the case handling process. This situation demonstrates that law enforcement against cybercrime requires cross-national coordination, which is not always easy to achieve [33].

The process of establishing evidence in cybercrime also presents its own complexities because it relies on invisible digital evidence. Collecting and analyzing digital evidence requires special procedures to ensure the validity and integrity of the data. Errors in this process can impact the strength of evidence in court. Furthermore, the easily modified

nature of digital data adds to the challenge of ensuring the authenticity of the evidence presented [2]. This situation demonstrates that the evidentiary system in criminal law needs to adapt to the characteristics of evidence in the digital space.

Coordination between law enforcement agencies also impacts the effectiveness of cybercrime handling. Case handling often involves various institutions with different authorities, such as the police, relevant ministries, and technology regulatory agencies. Differences in procedures and working mechanisms between agencies can create obstacles in the case handling process. The need for integrated coordination is crucial to ensure that each stage of law enforcement can run effectively. This demonstrates that cybercrime law enforcement requires a coordinated institutional approach [7].

The level of digital literacy in the community also indirectly impacts the effectiveness of law enforcement. Individuals with a poor understanding of digital security tend to be more vulnerable to crime. This situation increases the number of cases that law enforcement must handle. Furthermore, a lack of public awareness in reporting cybercrime also impacts the law enforcement process. This dynamic demonstrates that cybercrime prevention efforts depend not only on the authorities but also on public participation in maintaining digital security [34].

Rapid technological developments create a gap between digital innovation and regulatory and law enforcement capacity. Criminals can quickly adopt new technologies to develop more complex modus operandi. Meanwhile, the adaptation process within the legal system tends to be slower due to the lengthy formal procedures required. This imbalance creates space for perpetrators to exploit to commit crimes with varying levels of risk [35]. This phenomenon demonstrates that technological dynamics have direct implications for the effectiveness of law enforcement.

The interaction between technological, institutional, and regulatory factors demonstrates that the challenges facing law enforcement against cybercrime are multidimensional. Barriers to identifying perpetrators, limited resources, and jurisdictional complexity interact to shape conditions that influence the effectiveness of case handling. From a criminological perspective, this situation can be analyzed as an imbalance between crime opportunities and oversight capacity. This pattern suggests that law enforcement against cybercrime requires an approach that focuses not only on legal aspects but also on strengthening technological and institutional capacity to address the dynamics of digital crime.

3.2 Discussion

Theoretical Implications

This study contributes to the development of cybercriminology by reinforcing its central assumption that cybercrime emerges from the interaction between offenders, technological systems, and digital environments. The findings demonstrate that cybercrime in Indonesia cannot be sufficiently explained by traditional criminological theories alone, but requires an integrated cybercriminological framework that accounts for the fluid, borderless, and technologically mediated nature of criminal behavior in cyberspace.

From the perspective of Routine Activity Theory proposed by Cohen and Felson (1979) in [24], the findings support the idea that cybercrime occurs through the convergence of motivated offenders, suitable targets, and weak guardianship. However, this study extends the theory by showing that guardianship in digital environments is not limited to physical supervision, but also includes technological protections such as encryption systems, platform security mechanisms, and user-based digital awareness. This indicates that the concept of guardianship must be redefined within cyber contexts.

In relation to Rational Choice Theory, the results support the assumption that offenders engage in cybercrime after evaluating risks and potential benefits. Nevertheless, this study expands the theory by demonstrating that such rational calculations are significantly influenced by technological conditions that reduce perceived risks, particularly through anonymity tools, virtual private networks, and cross-border digital accessibility. As a result, rational decision-making in cybercrime becomes more dynamic and technologically conditioned compared to conventional crime settings.

Furthermore, this study supports and extends Space Transition Theory proposed by Jaishankar (2008) as cited in [36] by showing that offenders actively shift between physical and multiple digital spaces to exploit structural vulnerabilities. The findings indicate that cybercriminal behavior is not static but highly adaptive, allowing offenders to transition across platforms and jurisdictions to avoid detection and sustain illicit activities.

Overall, this study strengthens cybercriminology as an emerging interdisciplinary field by demonstrating that cybercrime must be understood through the integration of behavioral, technological, and structural perspectives. It confirms that existing criminological theories remain relevant, but require conceptual expansion to fully explain the complexity of crime in digital societies.

Legal Implications

The findings of this study have significant legal implications for the regulation and enforcement of cybercrime in Indonesia, particularly in relation to the adequacy of the Information and Electronic Transactions Law (UU ITE) as the primary legal framework governing digital offenses. Although UU ITE provides a foundational basis for cybercrime regulation, its implementation increasingly faces challenges due to the rapid evolution and sophistication of cybercriminal activities in digital environments. This indicates a growing normative gap between statutory legal provisions and the dynamic characteristics of cybercrime.

One key implication is the limited adaptability of existing legal instruments in addressing emerging forms of cybercrime, particularly offenses involving cross-border operations, anonymity technologies, and rapidly evolving digital platforms. In this context, legal norms tend to be reactive rather than anticipatory, which reduces their effectiveness in responding to new modus operandi of cyber offenders. Similar concerns regarding the rigidity of cyber law frameworks in adapting to technological change have been noted in previous studies on cybercrime regulation [6].

Furthermore, the study highlights a significant challenge in the evidentiary framework for cybercrime prosecution. Digital evidence requires strict procedural standards

to ensure authenticity, integrity, and admissibility in court proceedings. However, the current legal framework does not fully accommodate the technical complexity of digital forensic processes, creating difficulties in proving cybercrime cases beyond a reasonable doubt. This aligns with findings that emphasize the need for stronger legal integration of digital forensic standards in criminal proceedings [2].

Another important implication relates to jurisdictional limitations in handling transnational cybercrime. The borderless nature of digital offenses creates conflicts of jurisdiction, especially when perpetrators, victims, and digital infrastructure are located in different countries. Although international cooperation mechanisms exist, their implementation remains limited and inconsistent, thereby weakening cross-border law enforcement effectiveness. This reflects broader challenges identified in global cyber law enforcement cooperation frameworks.

Overall, these findings suggest that Indonesia's current cyber law framework requires substantial strengthening toward a more adaptive, technology-responsive, and internationally coordinated legal system. Reform efforts should not only focus on expanding substantive legal provisions within UU ITE, but also on improving procedural mechanisms for digital evidence handling and enhancing international cooperation in cybercrime enforcement.

Policy Implications

The findings of this study have important policy implications for strengthening cybercrime prevention and enforcement strategies in Indonesia. First, law enforcement institutions such as the police and other relevant agencies need to enhance their technological capabilities, particularly in digital forensics, cyber monitoring systems, and real-time threat detection. Given the increasingly sophisticated nature of cybercrime, traditional investigative approaches are no longer sufficient and must be supported by advanced technological infrastructure and specialized human resources.

Second, the National Cyber and Crypto Agency (BSSN) plays a critical role in strengthening national cybersecurity resilience. The results of this study indicate the need for a more integrated cyber defense system that connects government institutions, private sector platforms, and digital service providers. Strengthening coordination mechanisms among these stakeholders is essential to ensure a rapid response to cyber threats and reduce systemic vulnerabilities in digital ecosystems.

Third, from a preventive policy perspective, the government should prioritize the development of comprehensive digital literacy programs for the public. The findings show that user vulnerability remains one of the main entry points for cybercrime, particularly in cases involving phishing, social engineering, and online fraud. Therefore, public awareness campaigns, education programs, and school-based digital security curricula are essential to reduce exposure to cyber risks and strengthen individual-level digital resilience.

Furthermore, policy strategies should shift from reactive enforcement to proactive prevention. This includes the development of early warning systems, predictive cyber threat analysis, and stronger collaboration between public institutions and private digital platforms.

Such an approach allows for more effective identification and mitigation of cyber threats before they escalate into large-scale incidents.

Overall, these policy implications highlight the need for a holistic cybersecurity governance framework in Indonesia that integrates institutional capacity building, technological advancement, and public digital literacy. Strengthening synergy between law enforcement agencies, BSSN, and the broader public is essential to building a more resilient digital society capable of responding to evolving cybercrime threats.

4. CONCLUSION

This study concludes that the development of digital technology does not solely drive the increasing trend of cybercrime in Indonesia, but is also shaped by the interaction of individual, structural, and institutional factors within cyberspace. Through a cybercriminology perspective, cybercrime can be understood as a dynamic social phenomenon influenced by offender rationality, opportunity structures embedded in digital systems, and limitations in oversight and regulatory mechanisms. These dynamics indicate a transformation of crime patterns from conventional forms to more complex, flexible, anonymous, and transnational cyber-based offenses, requiring an integrated analytical framework that combines technological and social dimensions.

The findings of this study have important theoretical and practical implications. Theoretically, this research contributes to the development of cybercriminology by emphasizing the interaction between offenders, technology, and the digital environment as a unified analytical framework for understanding cybercrime. Practically, the results provide insights for law enforcement agencies and policymakers in designing more effective cybercrime prevention strategies that integrate technical capacity, institutional strengthening, and social awareness.

This study is subject to several limitations. It employs a normative juridical approach based on secondary data, which limits the analysis to conceptual and legal interpretation rather than empirical validation. In addition, the study focuses exclusively on the Indonesian context, without comparative analysis with other jurisdictions, thereby limiting the generalizability of the findings in a global context.

Future research is recommended to adopt empirical approaches involving primary data collection, such as interviews with law enforcement officials or case-based analysis, to strengthen the robustness of findings. Comparative studies across countries are also suggested to identify best practices in cybercrime management. Furthermore, future studies may explore strategies for enhancing digital literacy and institutional capacity as key components of cybercrime prevention. Overall, this study contributes to the growing body of knowledge on cybercrime and provides a foundation for understanding crime dynamics in the digital era.

REFERENCES

[1] M. F. Imran, “Preventing and Combating Cybercrime in Indonesia,” *Int. J. Cyber Criminol.*, vol. 17, no. 1, pp. 223–235, 2023, doi: 10.5281/zenodo.4766614.

[2] M. A. Sunggara and S. Hariansah, “Challenges and Threats of Cybercrime in Indonesia: A Review of Legal and Information Technology Aspects Related to Ransomware Attacks on Indonesia’s National

Data Center," *Pakistan J. Criminol.*, vol. 16, no. 04, pp. 955–964, 2024.

[3] S. T. Cahyono, W. Erni, and T. Hidayat, "Rekonstruksi Hukum Pidana terhadap Kejahatan Siber (Cyber Crime) dalam Sistem Peradilan Pidana Indonesia," *DJH Dame J. Huk.*, vol. 1, no. 1, pp. 111–133, 2025.

[4] J. M. Butarbutar, "Revolusi Digital dan Tantangan Kriminologis : Analisis terhadap Tren Kriminalitas dalam Era Digitalisasi," *Media Huk. Indones.*, vol. 2, no. 6, pp. 145–150, 2025, doi: https://doi.org/10.5281/zenodo.15493512.

[5] T. Nugroho and B. Soesatyo, "Problems of Cyber Law Enforcement Against Cyber Crimes Using Virtual Private Network Technology in Indonesia," *J. Greenation Sos. dan Polit.*, vol. 3, no. 4, pp. 713–721, 2026, doi: https://doi.org/10.38035/jgsp.v3i4.

[6] D. Widijowati, "Legal Complexity in Dealing with Cyber Crime in Indonesia," *Res. Horiz.*, vol. 2, no. 6, pp. 597–606, 2022, [Online]. Available: https://journal.lifescifi.com/index.php/RH/index

[7] I. Anwary, "The Role of Public Administration in combating cybercrime : An Analysis of the Legal Framework in Indonesia," *Int. J. Cyber Criminol.*, vol. 16, no. 2, pp. 216–227, 2022, doi: 10.5281/zenodo.4766577.

[8] S. D. Ganjar, "Urgensi Pembaruan Hukum Pidana dalam Menanggulangi Kejahatan Siber : Tinjauan Kritis Terhadap Kesesuaian KUHP Nasional dan Perubahan UU ITE," *Locus J. Acad. Lit. Rev.*, vol. 4, no. 3, pp. 197–208, 2025.

[9] R. G. Sihombing, S. Fattah, D. A. K. Nasution, R. Rosmalinda, and A. Hafizah, "Cyber Extortion as a Cybercrime in Indonesian Criminal Law : Normative Analysis and Legal Protection for Victims," *J. Law Perspect. Rev.*, vol. 2, no. 1, pp. 9–16, 2026, [Online]. Available: journal.catalystindo.org

[10] I. F. Edrisy and F. Rozi, "Penegakan Hukum terhadap Pelaku Pengancam Pornografi (Studi Kasus Polres Lampung Utara)," *J. Huk. Leg.*, vol. 1, no. 2, pp. 98–108, 2021.

[11] C. Tania and J. Gidalty, "Strategi Penuntutan Kejahatan Siber dengan Artificial Intelligence di Era Digital," *J. Ilmu Huk. dan Sos.*, vol. 2, no. 3, pp. 1–19, 2024, [Online]. Available: https://journal.stekom.ac.id/index.php/Hakim

[12] J. Cristina and I. Manalu, "Analisis Peran Alat Bukti dan Keterangan Saksi dalam Menentukan Keputusan Pengadilan Pidana," *J. Kaji. Huk. dan Kebijak. Publik*, vol. 3, no. 1, pp. 245–263, 2025, [Online]. Available: https://jurnal.kopusindo.com/index.php/jkhkp

[13] A. Nugroho and A. A. Chandrawulan, "Research synthesis of cybercrime laws and COVID - 19 in Indonesia : lessons for developed and developing countries," *Secur. J.*, pp. 1–29, 2022, doi: 10.1057/s41284-022-00357-y.

[14] R. Hukom and M. H. Setiadi, "Pengaruh Media Sosial terhadap Pola Kejahatan di Era Digital: Studi Kriminologi dengan Pendekatan Netnografi," *Perkara J. Ilmu Huk. dan Polit.*, vol. 3, no. 1, pp. 750–768, 2025, doi: 10.51903/perkara.v3i1.2353.

[15] A. M. R. Thomas and H. Y. Anggraeni, "Cybercrime dan Media Sosial Analis Hukum terhadap Tren Peningkatan Tindak Pidana di Era Digital," *Rewang Rencang J. Huk. Lex Gen.*, vol. 6, no. 7, pp. 1–22, 2025, [Online]. Available: https://jhlg.rewangrencang.com/

[16] D. P. Sari, Y. Probowati, M. P. Elisabeth, and A. Ayuni, "The use of criminal profiling in determining typology of conventional offender and cyber offender : systematic literature review," *J. Psikol. Tabularasa*, vol. 19, no. 1, pp. 1–17, 2024, doi: http://doi.org/10.26905/jpt.v19.i1.12154.

[17] G. R. A. Sihombing and B. Hermanto, "Dinamika Kebijakan Penegakan Hukum terhadap Pemanfaatan Kecerdasan Buatan dalam Kejahatan Siber di Indonesia," *J. Media Akad.*, vol. 4, no. 1, pp. 1–18, 2026.

[18] M. S. F. Rahman, "Kajian Kriminologis terhadap Motif dan Modus Operandi Tindak Pidana Perubahan Data di Indonesia," *HARISA J. Hukum, Syariah, dan Sos.*, vol. 02, no. 1, pp. 81–95, 2025.

[19] R. D. N. I. Sari, "Pengaruh Transformasi Sistem Keamanan dan Penggunaan Teknologi Baru terhadap Serangan Siber pada Data Nasabah," Institut Agama Islam Negeri Curup, 2025.

[20] S. M. T. Situmeang and K. Meilan, "The Evolution of Crime and Punishment : Challenges in Law Enforcement and Modern Penology," *Res Nullius Law J.*, vol. 7, no. 2, pp. 87–97, 2025, [Online]. Available: http://ojs.unikom.ac.id/index.php/law

[21] D. Malian, "Penanganan dan Tantangan Cybercrime di Era Digital Perspektif Kriminologi," *Innov. J. Soc. Sci. Res.*, vol. 4, no. 6, pp. 7048–7056, 2024, [Online]. Available: https://j-innovative.org/index.php/Innovative%0APenanganan

[22] R. Pangestu and S. Riyanta, "Perdagangan Manusia Bermodus Pekerjaan Ilegal : Nasib Pekerja Migran Indonesia di Kamboja," *SENTRI J. Ris. Ilm.*, vol. 4, no. 11, pp. 3616–3635, 2025, [Online]. Available: ejournal.nusantaraglobal.ac.id/index.php/sentri

[23] D. Khariri, R. Rohayu, and U. Ufran, "Anak Sebagai Pelaku Tindak Pidana Pencurian Dengan Kekerasan," *J. Commer. Law*, vol. 5, no. 2, pp. 309–326, 2025, doi: https://doi.org/10.29303/commercelaw.v5i2. 7854.

[24] T. J. Holt, R. Leukfeldt, and S. Van De Weijer, "An Examination of Motivation and Routine Activity Theory to Account for Cyberattacks Against Dutch Web Sites," *Crim. Justice Behav.*, vol. 47, no. 4, pp. 487–505, 2020, doi: 10.1177/0093854819900322.

[25] E. R. Leukfeldt and M. Yar, "Applying Routine Activity Theory to Cybercrime : A Theoretical and Empirical Analysis," *Deviant Behav.*, vol. 37, no. 3, pp. 263–280, 2016, doi: 10.1080/01639625.2015.1012409.

[26] A. S. P. Putra, V. I. Cornelis, F. Hamdani, and V. N. Paramitha, "Pengaruh Penggunaan Media Sosial Terhadap Peningkatan Tindak Pidana Kejahatan Siber (Cyber) di Kota Balikpapan," *J. Evid. Law*, vol. 4, no. 3, pp. 2232–2241, 2025, [Online]. Available: https://jurnal.erapublikasi.id/index.php/JEL

[27] V. A. Anjani, "Cyberbullying dan Dinamika Hukum di Indonesia : Paradoks Ruang Maya dalam Interaksi Sosial di Era Digital," *Staatsr. J. Huk. Kenegaraan dan Polit. Islam*, vol. 4, no. 1, pp. 1–28, 2024.

[28] V. F. Purba, R. B. L. Batu, R. B. B. Perangin-Angin, and M. Ibrahim, "Dampak Perubahan Teknologi Komunikasi terhadap Peningkatan Kejahatan Sosial: Studi Kasus Penggunaan Media Sosial di Era Digital," *Indones. J. Islam. Jurisprudence,Economic Leg. Theory*, vol. 1, no. 3, pp. 477–485, 2023, [Online]. Available: https://shariajournal.com/index.php/IJIJEL

[29] W. Wibowo, M. S. Imam, A. Munawar, and H. Hidayatullah, "Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia," *Rewang Rencang J. Huk. Lex Gen.*, vol. 5, no. 7, pp. 1–15, 2024, [Online]. Available: https://jhlg.rewangrencang.com/

[30] Z. K. Kadir, "Kejahatan Berbasis Identitas Digital : Menggagas Kebijakan Kriminal untuk Dunia Metaverse," *JULIA J. Litigasi Amsir*, vol. 12, no. 2022, pp. 124–137, 2025.

[31] A. R. Widianingrum, "Analisis Implementasi Kebijakan Hukum terhadap Penanganan Kejahatan Siber di Era Digital," *J. IURIS Sci.*, vol. 2, no. 2, pp. 90–102, 2024, [Online]. Available: https: //journal.merassa.id/index.php/JIS

[32] M. A. Azis, S. Purwanda, M. Darwis, K. Kairuddin, and B. Tijjang, "Tindak Pidana Judi Online Sebagai Kejahatan Siber : Analisis Normatif Terhadap Efektivitas Regulasi Di Indonesia," *Innov. J. Soc. Sci. Res.*, vol. 5, no. 4, pp. 3912–3928, 2025, [Online]. Available: https://j-innovative.org/index.php/Innovative

[33] D. R. Banjarani and M. A. Rahmadhani, "Kejahatan Cyber Sebagai Kejahatan Lintas Negara : Penegakan Hukum dan Penanggulangan Kejahatan Cyber dalam Perspektif Hukum Pidana Internasional," *Yustitia Tirtayasa*, vol. 4, no. 4, pp. 144--164, 2024, doi: http://dx.doi.org/10.51825/yta.v4i4.29046.

[34] M. H. Nevoso, W. A. Hidaya, K. Sukarna, M. Junaidi, and C. T. A. Sasti, "Perlindungan Hukum Korban Phishing: Analisis Kriminologi dan Efektivitas Regulasi di Indonesia Legal," *J. Jurid.*, vol. 4, no. 1, pp. 1–13, 2026, doi: https://doi.org/10.26623/jj.v4i1.12221.

[35] P. S. Irawan and D. P. Lestarika, "Kejahatan Transnasional Terorganisasi di Era Digital: Analisis Tren Kejahatan Siber dan Perdagangan Manusia Tahun 2025-2026," *JURRISH J. Ris. Rumpun Ilmu Sos. Polit. dan Hum.*, vol. 5, no. 2, pp. 1–13, 2026.

[36] M. F. Ihsan and M. Zaky, "Analisis Space Transition Theory Terhadap Normalisasi Konten Pornografi Pada Platform Youtube," *IKRAITH-HUMANIORA*, vol. 8, no. 2, pp. 297–308, 2024, doi: https://doi.org/10.37817/ikraith-humaniora.v8i2.