JURNAL ILMIAH DUNIA HUKUM
Volume 10 Issue 2 April 2026
ISSN Print: 2528-6137 | ISSN Online: 2721-0391

Digital Shadows: A Criminological Analysis of Cybercrime and Law Enforcement Challenges in Indonesia's Technological Disruption Era

Sri Wulandari[1], Farisha Dian Prabaningtyas[2]
[1,2] *Faculty of Law, University of August 17, 1945 Semarang, Indonesia*
* *Correspondence e-mail: Ndari904@gmail.com*

Submission
2026-Mar-31
Review
2026-Apr-20
Accepted
2026-Apr-22
Published
2026-Apr-30

Abstract

This study examines the phenomenon of cybercrime from a criminological perspective within the broader context of technological disruption characterized by the rapid advancement of information and communication technologies. The massive digital transformation has not only reshaped social interaction and economic activities but has also generated new forms of crime that are non-conventional, anonymous, and transnational in nature. Cybercrime presents significant challenges to legal systems, as it produces multidimensional impacts ranging from financial losses to psychological harm and threats to national security. This research employs a normative legal (doctrinal) method using statutory, conceptual, and comparative approaches, supported by an extensive literature review of primary, secondary, and tertiary legal sources. The findings reveal that cybercrime is driven by a combination of economic motives, social pressures, technological opportunities, and weaknesses in regulatory enforcement and digital supervision. From a criminological standpoint, this phenomenon can be explained through major theoretical frameworks, including Routine Activity Theory, Strain Theory, Differential Association Theory, Social Control Theory, and Rational Choice Theory. These theories collectively demonstrate that cybercrime emerges due to the convergence of motivated offenders, suitable targets, and the absence of capable guardians in digital environments, further exacerbated by structural inequalities and evolving technological capabilities. In the Indonesian context, cybercrime regulation has been established through several legal instruments, including the Law on Electronic Information and Transactions, the Personal Data Protection Law, and Government Regulations on Electronic System Implementation. However, the effectiveness of law enforcement remains limited due to challenges such as inadequate human resources, lack of advanced digital forensic capabilities, jurisdictional complexities, and evidentiary constraints. This study contributes to the existing literature by integrating criminological analysis with legal evaluation, highlighting the need for a multidisciplinary approach. It argues that effective prevention and mitigation of cybercrime require synergy between legal frameworks, criminological insights, and technological innovation, alongside strengthening digital literacy and institutional capacity to ensure a resilient and sustainable digital security system.

Keywords: *Cybercrime; Criminology; Law Enforcement*

How to Cite: Sri Wulandari, Farisha Dian Prabaningtyas: *"Digital Shadows : A Criminological Analysis of Cybercrime and Law Enforcement Challenges in Indonesia's Technological Disruption Era" Jurnal Ilmiah Dunia Hukum*, 10 no. 2 (2026): 81-97. DOI: 10.35973/jidh.xxxxxx

ISSN Print: 2528-6137 ISSN Online: 2721-0391

1. Introduction

The rapid development of information and communication technologies has fundamentally transformed the structure of modern society, reshaping patterns of interaction, economic transactions, governance, and social behavior. The emergence of digital ecosystems has created unprecedented opportunities for efficiency and connectivity; however, it has simultaneously generated new forms of criminality that operate beyond traditional legal frameworks. Among these emerging threats, cybercrime has become one of the most complex and rapidly evolving forms of transnational crime, posing serious challenges to both national and international legal systems.[1]

Cybercrime is generally understood as any unlawful act committed through or against computer systems, networks, or digital data. According to the United Nations Office on Drugs and Crime (UNODC), cybercrime encompasses a broad range of activities, including unauthorized access to systems (hacking), data interference, identity theft, online fraud, and cyber-enabled offenses such as digital harassment and financial scams.[2] The defining characteristics of cybercrime anonymity, borderless operation, and technological dependency distinguish it from conventional crime and complicate both its detection and prosecution.[3] Unlike traditional crimes, cybercrime can be executed remotely without physical presence, enabling perpetrators to target victims across multiple jurisdictions simultaneously.

In Indonesia, the escalation of cybercrime incidents reflects the increasing vulnerability of digital infrastructures and the growing dependence of society on online systems. Data from the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara/BSSN) indicates that hundreds of millions of cyberattacks are recorded annually, including phishing, malware distribution, ransomware, and

[1] United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (United Nations, 2013).
[2] Ibid.
[3] Susan W Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger, 2010).

data breaches.[4] These incidents not only cause substantial financial losses but also undermine public trust in digital systems, disrupt economic activities, and threaten national security. High-profile cases, such as large-scale data leaks and the proliferation of illegal online lending platforms, further illustrate the systemic weaknesses in cybersecurity governance and regulatory enforcement.

From a criminological perspective, cybercrime represents a transformation in the nature of criminal behavior, where technological advancement intersects with social, economic, and psychological factors. Traditional criminological theories remain relevant in explaining cybercriminal behavior, albeit with contextual adaptation to digital environments. Routine Activity Theory, for instance, posits that crime occurs when a motivated offender encounters a suitable target in the absence of capable guardianship.[5] In cyberspace, this convergence is facilitated by weak security systems, widespread digital exposure, and limited monitoring mechanisms. Similarly, Strain Theory explains how socio-economic pressures and inequality may drive individuals toward cybercrime as an alternative means of achieving financial or social goals.[6]

Moreover, Differential Association Theory emphasizes that criminal behavior is learned through interaction with deviant communities, a phenomenon that is increasingly evident in online forums and hacker networks.[7] Social Control Theory further suggests that weakened social bonds and reduced institutional oversight in digital spaces contribute to the rise of cybercriminal activities.[8] In addition, Rational Choice Theory highlights that individuals engage in cybercrime after weighing the perceived benefits against the risks, which are often minimal due to limited law enforcement capacity and low probability of

[4] Badan Siber dan Sandi Negara (BSSN), *Laporan Statistik Serangan Siber Nasional Tahun 2023* (BSSN, 2023).
[5] Lawrence E Cohen and Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* 44, no. 4 (1979): 588–608.
[6] Robert K Merton, "Social Structure and Anomie," *American Sociological Review* 3, no. 5 (1938): 672–682.
[7] Edwin H Sutherland, *Principles of Criminology* (4th ed., J.B. Lippincott, 1947).
[8] Travis Hirschi, *Causes of Delinquency* (University of California Press, 1969).

detection.[9] These theoretical frameworks collectively provide a comprehensive understanding of the motivations and dynamics underlying cybercrime in the digital era.

Despite the growing body of literature on cybercrime, existing studies often focus on either technical aspects of cybersecurity or general legal frameworks without adequately integrating criminological analysis with legal enforcement challenges. In the Indonesian context, research tends to emphasize normative legal provisions, such as the Law on Electronic Information and Transactions (ITE Law) and the Personal Data Protection Law, while insufficient attention is given to the criminological dimensions that influence the effectiveness of these regulations. This gap highlights the need for an interdisciplinary approach that combines legal analysis with criminological insights to better understand and address cybercrime.

Furthermore, although Indonesia has established a regulatory framework to address cybercrime including Law No. 11 of 2008 as amended, Law No. 27 of 2022 on Personal Data Protection, and Government Regulation No. 71 of 2019 significant challenges remain in implementation. These include limited technical expertise among law enforcement officials, inadequate digital forensic infrastructure, jurisdictional constraints in cross-border cases, and difficulties in gathering and validating electronic evidence.[10] As a result, the enforcement of cybercrime laws often fails to keep pace with the rapid evolution of criminal techniques and technologies.

This study seeks to address these gaps by examining cybercrime through a criminological lens while simultaneously evaluating the effectiveness of law enforcement mechanisms in Indonesia. The central legal issue of this research

[9] Derek B Cornish and Ronald V Clarke, *The Reasoning Criminal: Rational Choice Perspectives on Offending* (Springer, 1986).

[10] R Nugroho and I M Putri, "Strategi Penegakan Hukum terhadap Kejahatan Siber di Indonesia," *Jurnal Hukum dan Pembangunan* 51, no. 2 (2021): 273–290.

concerns the extent to which existing legal frameworks are capable of responding to the evolving nature of cybercrime and the role of criminological theories in enhancing law enforcement strategies. Accordingly, this research aims to (1) analyze the characteristics and typologies of cybercrime, (2) examine the criminological factors driving cybercriminal behavior, and (3) evaluate the effectiveness of Indonesia's legal framework in addressing cybercrime.

By integrating doctrinal legal analysis with criminological perspectives, this study offers a more holistic understanding of cybercrime as both a legal and social phenomenon. It argues that effective prevention and mitigation of cybercrime require not only robust legal instruments but also a deeper understanding of the behavioral and structural factors that enable such crimes. Therefore, strengthening digital literacy, enhancing institutional capacity, and fostering international cooperation are essential components of a comprehensive cybercrime governance strategy.

2. Research Method

This study employs a normative legal research method (doctrinal research), which is primarily concerned with the analysis of legal norms, principles, and doctrines governing cybercrime and its enforcement. Normative legal research is used to examine the coherence, adequacy, and effectiveness of existing legal frameworks in addressing contemporary legal issues arising from technological disruption, particularly in the context of cybercrime.[11]

The research adopts several approaches to ensure a comprehensive legal analysis. First, the statutory approach is utilized to analyze relevant legislation governing cybercrime in Indonesia, including Law No. 11 of 2008 on Electronic Information and Transactions as amended, Law No. 27 of 2022 on Personal Data Protection, and Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions. These legal instruments are examined to

[11] Peter Mahmud Marzuki, *Penelitian Hukum* (17th ed., Prenada Media, 2022).

assess their scope, limitations, and applicability in addressing cybercrime phenomena.

Second, the conceptual approach is applied to explore and clarify key legal and criminological concepts related to cybercrime. This approach involves the examination of doctrines and theoretical frameworks, particularly those derived from criminological theories such as Routine Activity Theory, Strain Theory, Differential Association Theory, Social Control Theory, and Rational Choice Theory. Through this approach, the study seeks to construct a theoretical foundation that explains the underlying causes and dynamics of cybercriminal behavior.

Third, a comparative approach is employed to compare Indonesia's legal framework with international standards and practices in cybercrime regulation and enforcement. This includes reference to international instruments and guidelines, as well as comparative insights from other jurisdictions, in order to identify gaps and potential areas for legal reform. The comparative analysis is essential in understanding how different legal systems respond to the challenges of cybercrime, particularly in cross-border contexts.

The data used in this research consist of secondary legal materials, which include primary legal materials (statutes, regulations, and official legal documents), secondary legal materials (academic journals, books, and scholarly articles), and tertiary legal materials (legal dictionaries, encyclopedias, and reports from international organizations). Data collection is conducted through an extensive literature review, focusing on authoritative and up-to-date sources relevant to cybercrime and criminology.

The analysis of legal materials is carried out using a prescriptive analytical method, which aims not only to describe existing legal norms but also to provide normative evaluations and recommendations. This approach enables the study to assess whether current legal frameworks are adequate in addressing

cybercrime and to propose improvements based on doctrinal reasoning and criminological insights. By integrating legal analysis with criminological perspectives, this research seeks to contribute to the development of a more effective and adaptive legal framework for combating cybercrime in Indonesia.

3. Research Results and Discussion

3.1. Conceptualization and Evolution of Cybercrime in the Digital Era

The conceptualization of cybercrime has evolved significantly alongside the rapid development of digital technologies and global connectivity. In contemporary legal and criminological discourse, cybercrime is no longer limited to simple unauthorized access or data theft but encompasses a wide spectrum of criminal activities that exploit digital infrastructures, information systems, and online platforms. The transformation of cybercrime reflects a broader shift in the nature of criminality, where traditional boundaries of space, time, and jurisdiction are increasingly blurred.

Cybercrime can be broadly defined as any unlawful act committed using or targeting computer systems, networks, or digital data. However, modern scholarship distinguishes between cyber-dependent crimes and cyber-enabled crimes. Cyber-dependent crimes refer to offenses that can only be committed through digital systems, such as hacking, malware distribution, and denial-of-service attacks. In contrast, cyber-enabled crimes are traditional offenses facilitated by digital technology, including online fraud, identity theft, and cyber harassment.[12] This distinction is essential in understanding the diverse typologies of cybercrime and their implications for legal regulation and enforcement.

The evolution of cybercrime is closely linked to the expansion of the digital economy and the increasing reliance on interconnected systems. The

[12] UNODC, *Comprehensive Study on Cybercrime* (United Nations, 2019).

proliferation of e-commerce, financial technology, and digital public services has created new opportunities for cybercriminals to exploit vulnerabilities. According to recent studies, the global cost of cybercrime continues to rise significantly, driven by sophisticated attack methods such as ransomware, phishing schemes, and data breaches.[13] These developments indicate that cybercrime is not merely a technological issue but a complex socio-legal phenomenon that requires interdisciplinary analysis.

One of the defining characteristics of cybercrime is its transnational nature. Unlike conventional crimes that are confined within territorial boundaries, cybercrime often involves actors, victims, and infrastructures located in different jurisdictions. This creates significant challenges for law enforcement agencies, particularly in terms of jurisdiction, evidence gathering, and international cooperation.[14] The borderless nature of cyberspace allows perpetrators to operate with relative impunity, exploiting differences in legal systems and enforcement capacities across countries.

Another critical aspect of cybercrime is its anonymity. The use of encryption technologies, virtual private networks (VPNs), and dark web platforms enables offenders to conceal their identities and evade detection. This anonymity not only complicates investigative processes but also lowers the perceived risk of engaging in criminal activities. From a criminological perspective, the reduced risk of detection significantly influences the decision-making process of offenders, reinforcing the applicability of rational choice theory in explaining cybercriminal behavior.

Furthermore, cybercrime is characterized by its scalability and potential for mass victimization. A single cyberattack can simultaneously affect thousands or even millions of users, as seen in large-scale data breaches and

[13] Accenture, *Cost of Cybercrime Study* (2023).
[14] Europol, *Internet Organised Crime Threat Assessment (IOCTA)* (2022).

distributed denial-of-service (DDoS) attacks.[15] This capacity for widespread impact distinguishes cybercrime from many traditional forms of crime and amplifies its social and economic consequences. The increasing frequency of such incidents highlights the urgent need for robust cybersecurity measures and effective legal responses.

In the Indonesian context, the conceptualization of cybercrime must also consider the socio-economic and technological landscape of the country. Rapid digitalization, coupled with varying levels of digital literacy, has created both opportunities and vulnerabilities. The widespread use of mobile technology and online platforms has facilitated economic growth but has also exposed individuals and institutions to cyber risks. Reports indicate that phishing, online fraud, and illegal digital lending schemes are among the most prevalent forms of cybercrime in Indonesia.[16] These phenomena demonstrate that cybercrime is deeply embedded in everyday digital practices and cannot be addressed solely through formal legal mechanisms.

Moreover, the evolution of cybercrime reflects the adaptive nature of criminal behavior. Cybercriminals continuously develop new techniques to bypass security systems and exploit emerging technologies, including artificial intelligence and cryptocurrency.[17] This dynamic environment requires legal frameworks to be flexible and responsive, capable of addressing both current and future threats. However, legal systems often struggle to keep pace with technological innovation, resulting in regulatory gaps and enforcement challenges.

From a doctrinal perspective, the conceptual ambiguity of cybercrime poses additional challenges. The absence of a universally accepted definition complicates the harmonization of legal frameworks and international

[15] ENISA, *Threat Landscape Report* (2023).
[16] Badan Siber dan Sandi Negara (BSSN), *Laporan Statistik Serangan Siber Nasional Tahun 2023*.
[17] INTERPOL, *Global Cybercrime Report* (2023).

cooperation. While national laws provide specific definitions and categorizations, variations across jurisdictions can hinder coordinated responses to transnational cybercrime. Therefore, a clear and comprehensive conceptual framework is essential for effective regulation and enforcement.

In light of these developments, it is evident that cybercrime must be understood as a multidimensional phenomenon that intersects law, technology, and society. Its conceptualization requires not only legal definitions but also criminological insights that explain the motivations, behaviors, and structural conditions underlying cybercriminal activities. By integrating these perspectives, this study provides a more nuanced understanding of cybercrime and its implications for law enforcement in Indonesia.

3.2. Criminological Theories Explaining Cybercrime

A comprehensive understanding of cybercrime requires a theoretical framework capable of explaining not only the occurrence of criminal acts but also the structural and behavioral conditions that facilitate them in digital environments. Classical criminological theories, when contextualized within cyberspace, remain highly relevant in explaining the dynamics of cybercriminal behavior. However, their application must be adapted to account for the unique characteristics of digital interaction, including anonymity, virtuality, and technological mediation.

Routine Activity Theory remains one of the most influential frameworks in explaining cybercrime. The theory posits that crime occurs when a motivated offender encounters a suitable target in the absence of capable guardianship.[18] In cyberspace, this convergence is significantly intensified. The digital environment offers an abundance of suitable targets, ranging

[18] Lawrence E Cohen and Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* 44, no. 4 (1979): 588–608.

from individual users to large-scale institutional databases. At the same time, the absence of effective guardianship manifested in weak cybersecurity systems, inadequate monitoring, and low user awareness creates an environment highly conducive to criminal activity.[19] Empirical studies indicate that organizations with weak cybersecurity protocols are disproportionately targeted by cybercriminals, reinforcing the applicability of this theory in modern contexts.[20]

Moreover, the concept of "capable guardianship" has evolved in the digital age to include not only human oversight but also technological safeguards such as firewalls, encryption, and intrusion detection systems.[21] The absence or inadequacy of these mechanisms significantly increases vulnerability, thereby creating opportunities for cybercrime. This highlights the need for a multidimensional approach to prevention that integrates both human and technological forms of guardianship.

Strain Theory provides a complementary perspective by focusing on the socio-economic factors that drive individuals toward cybercrime. According to this theory, individuals who experience a disjunction between societal goals and the legitimate means to achieve them may resort to illegitimate methods.[22] In the context of cybercrime, the relatively low barriers to entry and the high potential rewards make digital crime an attractive alternative for individuals experiencing economic hardship or social marginalization.[23] Recent studies have demonstrated a correlation between unemployment rates and the rise of cyber-enabled financial crimes, particularly in developing economies.[24]

---

[19] Europol, *Internet Organised Crime Threat Assessment (IOCTA)* (2022).
[20] ENISA, *Threat Landscape Report* (2023).
[21] OECD, *Digital Security Risk Management* (2020).
[22] Robert K Merton, "Social Structure and Anomie," *American Sociological Review* 3, no. 5 (1938): 672–682.
[23] World Bank, *Digital Development Report* (2021).
[24] UNODC, *Cybercrime Study Update* (2019).

The digital environment amplifies these pressures by providing accessible tools and platforms that facilitate criminal behavior. Online tutorials, hacking tools, and illicit marketplaces reduce the technical expertise required to commit cybercrime, thereby democratizing access to criminal opportunities.[25] This phenomenon illustrates how structural inequalities and technological accessibility intersect to produce new forms of criminal behavior.

Differential Association Theory further explains cybercrime as a learned behavior acquired through interaction with deviant peers. In digital spaces, this interaction is facilitated through online forums, encrypted communication channels, and dark web communities.[26] These platforms enable the dissemination of criminal knowledge, techniques, and values, creating a virtual subculture that normalizes cybercriminal activities.[27] Research indicates that individuals who actively participate in such communities are more likely to engage in cybercrime, as they are exposed to both the technical skills and the normative justifications for such behavior.[28]

The role of online communities in shaping criminal behavior cannot be underestimated. Unlike traditional criminal networks, digital communities operate across geographical boundaries and allow for rapid information exchange. This accelerates the learning process and enables the rapid evolution of cybercriminal techniques.[29] Consequently, law enforcement agencies face significant challenges in infiltrating and disrupting these decentralized networks.

Social Control Theory provides another critical lens for understanding cybercrime by emphasizing the role of social bonds in preventing deviant

[25] INTERPOL, *Global Cybercrime Report* (2023).
[26] Edwin H Sutherland, *Principles of Criminology* (4th ed., J.B. Lippincott, 1947).
[27] Europol, *IOCTA Report* (2022).
[28] Holt, T. J., *Cybercrime and Digital Deviance* (Routledge, 2016).
[29] Wall, D. S., *Cybercrime and Society* (2nd ed., Sage, 2017).

behavior. According to this theory, individuals are less likely to engage in criminal activities when they maintain strong attachments to family, educational institutions, and societal norms.[30] In digital environments, however, these social bonds are often weakened due to the absence of direct interpersonal interaction and the perceived detachment from real-world consequences. This detachment reduces the effectiveness of informal social controls, thereby increasing the likelihood of deviant behavior.[31]

In the Indonesian context, this weakening of social control is further exacerbated by uneven digital literacy and limited public awareness regarding ethical behavior in cyberspace. Research conducted by Indonesian scholars indicates that low levels of digital literacy significantly contribute to the normalization of deviant online behaviors, including online fraud, cyberbullying, and the misuse of personal data.[32] This condition reflects a broader structural issue in which rapid digital transformation is not accompanied by adequate social and educational adaptation.

The normalization of unethical digital practices also manifests in the widespread tolerance of minor cyber offenses, such as illegal streaming, data piracy, and online impersonation. These practices are often perceived as harmless, thereby reducing the moral barriers that typically prevent individuals from engaging in criminal behavior.[33] In this regard, strengthening digital ethics and promoting responsible online conduct are essential components of cybercrime prevention strategies.

Rational Choice Theory offers an additional explanatory framework by focusing on the decision-making processes of offenders. This theory assumes that individuals engage in criminal activities after evaluating the potential

[30] Travis Hirschi, *Causes of Delinquency* (University of California Press, 1969).
[31] ENISA, *Cybersecurity Culture Guidelines* (2022).
[32] R Nugroho and I M Putri, "Strategi Penegakan Hukum terhadap Kejahatan Siber di Indonesia," *Jurnal Hukum dan Pembangunan* 51, no. 2 (2021): 273–290.
[33] OECD, *Digital Security Behaviour Report* (2021).

benefits and risks associated with their actions.[34] In the context of cybercrime, the perceived benefits such as financial gain, anonymity, and minimal operational costs often outweigh the perceived risks, particularly in jurisdictions with limited law enforcement capacity.[35] Empirical evidence in Indonesia suggests that many cybercriminals exploit gaps in law enforcement and the slow pace of legal adaptation to technological change.[36]

The application of Rational Choice Theory is particularly relevant in understanding the professionalization of cybercrime. Organized cybercriminal groups operate in a manner similar to legitimate businesses, employing structured strategies, division of labor, and profit-oriented objectives.[37] In Indonesia, cases involving organized phishing syndicates and illegal online lending platforms demonstrate how cybercrime has evolved into a coordinated and economically driven activity.[38] This professionalization further complicates law enforcement efforts, as it requires advanced investigative techniques and cross-border cooperation.

In addition to classical theories, contemporary criminological perspectives have introduced the concept of "cyber opportunity structures," which emphasizes how digital infrastructures create new opportunities for crime.[39] The rapid expansion of internet access, mobile technology, and digital financial services in Indonesia has significantly increased these opportunities.[40] While such developments contribute to economic growth, they also expose users to greater cyber risks, particularly in the absence of adequate security awareness and institutional safeguards.

---

[34] Derek B Cornish and Ronald V Clarke, *The Reasoning Criminal: Rational Choice Perspectives on Offending* (Springer, 1986).
[35] Accenture, *Cost of Cybercrime Study* (2023).
[36] Badan Siber dan Sandi Negara (BSSN), *Laporan Statistik Serangan Siber Nasional Tahun 2023*.
[37] Europol, *Internet Organised Crime Threat Assessment (IOCTA)* (2022).
[38] Kementerian Komunikasi dan Informatika Republik Indonesia, *Laporan Penanganan Kejahatan Siber* (2023).
[39] Yar, M., *Cybercrime and Society* (2nd ed., Sage, 2017).
[40] World Bank, *Digital Development Report* (2021).

The integration of emerging technologies such as artificial intelligence, blockchain, and cryptocurrency has further expanded the scope of cybercrime by enabling more sophisticated and less detectable forms of criminal activity.[41] Indonesian regulatory institutions have acknowledged these challenges, particularly in relation to cryptocurrency-based fraud and digital financial crimes.[42] These developments illustrate that cybercrime is not only a product of individual motivation but also a consequence of technological evolution and systemic vulnerabilities within national infrastructures.

The integration of these theoretical perspectives provides a comprehensive framework for understanding cybercrime as a multidimensional phenomenon. Each theory contributes unique insights into the motivations, behaviors, and structural conditions that facilitate cybercrime. When combined, they reveal that cybercrime is driven by the interaction between individual rationality, social influences, economic pressures, and technological opportunities.

From a legal perspective, the application of criminological theories underscores the limitations of purely punitive approaches to cybercrime. While criminal sanctions are necessary, they are insufficient in addressing the root causes of cybercriminal behavior. Effective prevention requires a holistic approach that incorporates legal enforcement, technological innovation, and social intervention.[43] This includes strengthening cybersecurity infrastructure, enhancing digital literacy, and fostering international cooperation to address the transnational nature of cybercrime.

In the Indonesian context, the integration of criminological insights into legal policy remains limited. Existing legal frameworks primarily focus on

[41] World Economic Forum, *Global Cybersecurity Outlook* (2023).
[42] Otoritas Jasa Keuangan (OJK), *Laporan Tahunan Sektor Jasa Keuangan Digital* (2023).
[43] UNODC, *Cybercrime Strategy Report* (2020).

defining and penalizing cybercrime, with less emphasis on preventive measures informed by criminological analysis. Indonesian legal scholars argue that law enforcement strategies must be complemented by socio-legal approaches that address behavioral and structural factors underlying cybercrime.[44] This gap highlights the need for a more interdisciplinary approach that combines legal and criminological perspectives in order to develop more effective and adaptive strategies for combating cybercrime.

3.3. Factors and Motives Driving Cybercrime in Indonesia

The rapid escalation of cybercrime in Indonesia cannot be understood solely through legal or technological perspectives; rather, it must be examined through a multidimensional framework that integrates criminological, socio-economic, and institutional factors. Cybercrime emerges from the interaction between individual motivations, structural inequalities, technological accessibility, and weaknesses in legal enforcement. By situating these factors within the Indonesian context, it becomes evident that cybercrime is not merely a byproduct of digitalization, but also a reflection of broader systemic challenges.

One of the primary drivers of cybercrime is economic motivation. Financial gain remains the dominant incentive behind various forms of cybercrime, including phishing, online fraud, identity theft, and ransomware attacks.[45] In Indonesia, the proliferation of digital financial services, e-commerce platforms, and online banking systems has created lucrative opportunities for cybercriminals. The increasing reliance on digital transactions, particularly during and after the COVID-19 pandemic, has further expanded the attack surface for financially motivated crimes.[46] Empirical data from national institutions indicate that online fraud and phishing are

[44] Barda Nawawi Arief, *Kebijakan Hukum Pidana dalam Penanggulangan Cyber Crime* (Citra Aditya Bakti, 2018).
[45] Accenture, *Cost of Cybercrime Study* (2023).
[46] World Bank, *Digital Development Report* (2021).

among the most frequently reported cyber incidents, highlighting the economic dimension of cybercriminal activity.[47]

Economic inequality and unemployment also play a significant role in shaping cybercriminal behavior. From the perspective of Strain Theory, individuals who are unable to achieve financial stability through legitimate means may resort to cybercrime as an alternative pathway.[48] In Indonesia, disparities in income distribution and limited access to formal employment opportunities contribute to the emergence of cyber-enabled criminal activities, particularly among younger populations with basic technological skills.[49] The accessibility of online tools and platforms lowers the barriers to entry, enabling individuals with minimal technical expertise to engage in illicit activities.

In addition to economic factors, social influences significantly contribute to the growth of cybercrime. Differential Association Theory suggests that individuals learn criminal behavior through interaction with deviant peers.[50] In the Indonesian digital landscape, this learning process is facilitated by online communities, social media platforms, and encrypted communication channels that disseminate knowledge related to hacking, phishing, and other cyber offenses.[51] The existence of such communities creates an environment in which cybercrime is normalized and even incentivized, particularly when successful cases are publicly showcased.

Another critical factor is the rapid expansion of technology without corresponding growth in digital literacy. Indonesia has experienced significant digital transformation, with widespread internet penetration

[47] Badan Siber dan Sandi Negara (BSSN), *Laporan Statistik Serangan Siber Nasional Tahun 2023*.
[48] Robert K Merton, "Social Structure and Anomie," *American Sociological Review* 3, no. 5 (1938): 672–682.
[49] Bappenas, *Laporan Pembangunan Digital Indonesia* (2022).
[50] Edwin H Sutherland, *Principles of Criminology* (4th ed., J.B. Lippincott, 1947).
[51] INTERPOL, *Global Cybercrime Report* (2023).

and mobile device usage. However, this technological advancement is not always accompanied by adequate user awareness regarding cybersecurity risks.[52] Low levels of digital literacy make individuals more vulnerable to cyber threats, while also increasing the likelihood of participation in cybercrime, whether intentionally or unintentionally. For example, many users unknowingly engage in illegal activities such as data sharing, unauthorized access, or participation in fraudulent schemes due to a lack of understanding of legal consequences.[53]

The role of technological accessibility further amplifies the risk of cybercrime. The availability of hacking tools, malware kits, and tutorials on the internet has significantly reduced the technical barriers required to commit cyber offenses.[54] In Indonesia, the widespread use of affordable smartphones and internet access has democratized technology, enabling both positive and negative uses. While this accessibility contributes to economic growth, it also creates opportunities for cybercriminal activities, particularly in the absence of strong regulatory oversight.

Institutional weaknesses, particularly in law enforcement, constitute another major factor driving cybercrime. Despite the existence of legal frameworks such as the Electronic Information and Transactions Law and the Personal Data Protection Law, enforcement remains inconsistent and often ineffective.[55] Limited human resources, lack of specialized training in digital forensics, and inadequate technological infrastructure hinder the ability of law enforcement agencies to investigate and prosecute cybercrime cases.[56] Furthermore, the transnational nature of cybercrime complicates

[52] Kementerian Komunikasi dan Informatika, *Status Literasi Digital Indonesia* (2022).
[53] OECD, *Digital Security Behaviour Report* (2021).
[54] Europol, *Internet Organised Crime Threat Assessment (IOCTA)* (2022).
[55] Undang-Undang Nomor 11 Tahun 2008 tentang ITE jo. Undang-Undang Nomor 19 Tahun 2016.
[56] R Nugroho and I M Putri, "Strategi Penegakan Hukum terhadap Kejahatan Siber di Indonesia," *Jurnal Hukum dan Pembangunan* 51, no. 2 (2021): 273–290.

jurisdictional authority, making it difficult to apprehend offenders operating from outside Indonesia.

From the perspective of Rational Choice Theory, these enforcement gaps significantly influence the decision-making process of cybercriminals. When the perceived risk of detection and punishment is low, individuals are more likely to engage in criminal behavior.[57] In Indonesia, delays in legal processes and challenges in evidence collection contribute to the perception that cybercrime is a low-risk, high-reward activity.[58] This perception is reinforced by the relatively low rate of successful prosecutions in cybercrime cases.

Another important factor is the cultural and social perception of cybercrime. In some cases, minor cyber offenses are not viewed as serious crimes, particularly when they do not involve direct physical harm. This perception reduces the social stigma associated with cybercrime and may encourage individuals to engage in such activities.[59] The normalization of behaviors such as illegal downloading, account sharing, and online impersonation reflects a broader issue of digital ethics within society.

Furthermore, the emergence of organized cybercrime networks has transformed cybercrime into a structured and coordinated activity. In Indonesia, cases involving illegal online lending platforms and coordinated phishing operations demonstrate the existence of organized groups that operate systematically to exploit digital vulnerabilities.[60] These groups often employ division of labor, advanced technological tools, and cross-border operations, making them more difficult to detect and dismantle.

[57] Derek B Cornish and Ronald V Clarke, *The Reasoning Criminal: Rational Choice Perspectives on Offending* (Springer, 1986).
[58] Badan Siber dan Sandi Negara (BSSN), *Laporan Tahunan Keamanan Siber* (2023).
[59] ENISA, *Cybersecurity Culture Guidelines* (2022).
[60] Otoritas Jasa Keuangan (OJK), *Laporan Penanganan Pinjaman Online Ilegal* (2023).

The convergence of these factors economic incentives, social influences, technological accessibility, and institutional weaknesses demonstrates that cybercrime in Indonesia is a complex and multifaceted phenomenon. Addressing this issue requires a comprehensive approach that goes beyond traditional law enforcement. Preventive strategies must include improving digital literacy, strengthening cybersecurity infrastructure, enhancing legal enforcement capacity, and fostering collaboration between government agencies, private sector actors, and international organizations.

From a normative legal perspective, the identification of these factors is essential for formulating effective legal policies. Laws that focus solely on punishment without addressing underlying causes are unlikely to produce sustainable results. Therefore, integrating criminological insights into legal frameworks is crucial in developing a more adaptive and effective response to cybercrime in Indonesia.

3.4. Legal Framework, Law Enforcement Challenges, and Criminology-Based Prevention of Cybercrime in Indonesia

The regulation and enforcement of cybercrime in Indonesia cannot be examined in isolation between legal norms, institutional practices, and preventive strategies. Instead, these elements must be understood as an integrated system in which legal frameworks, enforcement mechanisms, and criminological approaches interact dynamically. This section therefore synthesizes the analysis of Indonesia's legal framework, the challenges in its enforcement, and criminology-based policy recommendations into a unified discussion.

Indonesia has established a relatively comprehensive legal framework to address cybercrime, primarily through Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), as amended by Law No. 19 of 2016 and Law No. 1 of 2024, Law No. 27 of 2022 on Personal Data Protection (PDP

Law), and Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions (PP PSTE).[61] These instruments collectively provide the normative basis for regulating unlawful acts in cyberspace, ranging from unauthorized access and data manipulation to online fraud and violations of personal data.

From a doctrinal perspective, the ITE Law represents a significant legal development in extending criminal law principles into the digital domain. However, its provisions have been widely criticized for their broad and ambiguous formulation, particularly regarding defamation and content-related offenses.[62] Such ambiguity creates legal uncertainty and raises concerns regarding potential misuse, thereby undermining the principle of legal certainty.[63] The PDP Law, on the other hand, reflects a progressive step toward protecting individual digital rights by introducing principles aligned with global standards, such as consent, accountability, and data minimization.[64] Nevertheless, its effectiveness remains dependent on enforcement mechanisms, including the establishment of an independent supervisory authority and the imposition of effective sanctions.[65]

Similarly, PP PSTE imposes obligations on electronic system providers to ensure data security and system reliability.[66] While this regulation is essential in strengthening cybersecurity governance, its implementation remains inconsistent, particularly among smaller institutions with limited technical

[61] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 2016 jo. Undang-Undang Nomor 1 Tahun 2024.
[62] Amnesty International, *Pasal-pasal Karet dalam UU ITE dan Dampaknya terhadap Kebebasan Berekspresi di Indonesia*(2020).
[63] Institute for Criminal Justice Reform (ICJR), *Reformulasi UU ITE* (2021).
[64] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
[65] Kementerian Komunikasi dan Informatika, *Pedoman Perlindungan Data Pribadi* (2023).
[66] Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

capacity.[67] This reveals a recurring gap between normative regulation and practical enforcement in Indonesia's cyber law regime.

The challenges in law enforcement further illustrate the limitations of the existing legal framework. One of the most significant obstacles is the limited capacity of law enforcement institutions, particularly in terms of human resources and technical expertise. Cybercrime investigations require specialized skills in digital forensics and data analysis, which are not yet uniformly available across regions.[68] In addition, the lack of advanced technological tools for evidence collection and analysis reduces the effectiveness of investigations and prosecutions.[69]

The complexity of digital evidence also poses serious challenges. Unlike conventional evidence, electronic evidence is highly volatile and requires strict procedural handling to ensure its admissibility in court.[70] The absence of standardized procedures and technical expertise often leads to procedural errors, weakening the legal position of prosecutors. Furthermore, judicial understanding of digital evidence remains limited, creating additional barriers in the adjudication process.

Jurisdictional constraints constitute another critical issue. Cybercrime frequently involves cross-border elements, making it difficult for national authorities to assert jurisdiction and enforce legal provisions.[71] Although Indonesia participates in international cooperation mechanisms, the lack of comprehensive legal harmonization and enforcement agreements limits their

[67] World Bank, *Digital Development Report* (2021).
[68] R Nugroho and I M Putri, "Strategi Penegakan Hukum terhadap Kejahatan Siber di Indonesia," *Jurnal Hukum dan Pembangunan* 51, no. 2 (2021): 273–290.
[69] INTERPOL, *Global Cybercrime Report* (2023).
[70] UNODC, *Cybercrime Study Update* (2019).
[71] Europol, *Internet Organised Crime Threat Assessment (IOCTA)* (2022).

effectiveness.[72] This condition creates opportunities for cybercriminals to exploit legal gaps across jurisdictions.

From a criminological perspective, these enforcement weaknesses contribute to the perception that cybercrime is a low-risk activity. Rational Choice Theory explains that individuals are more likely to engage in criminal behavior when the perceived benefits outweigh the risks.[73] In Indonesia, delays in legal processes, limited enforcement capacity, and low conviction rates reinforce this perception, thereby encouraging the persistence of cybercrime.

In addition, institutional fragmentation further reduces the effectiveness of law enforcement. Cybercrime prevention and response require coordination among multiple stakeholders, including law enforcement agencies, regulatory bodies, financial institutions, and private sector actors.[74] However, coordination mechanisms in Indonesia remain suboptimal, resulting in inefficiencies and overlapping responsibilities.

Given these limitations, it is evident that a purely punitive approach to cybercrime is insufficient. Criminological theories provide valuable insights into alternative strategies that emphasize prevention and structural reform. Routine Activity Theory suggests that reducing opportunities for cybercrime requires strengthening cybersecurity systems and increasing capable guardianship.[75] This includes the implementation of advanced technological safeguards and the enhancement of user awareness through public education.

[72] INTERPOL, *Global Cybercrime Report* (2023).
[73] Derek B Cornish and Ronald V Clarke, *The Reasoning Criminal: Rational Choice Perspectives on Offending* (Springer, 1986).
[74] OECD, *Digital Security Risk Management* (2020).
[75] Lawrence E Cohen and Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* 44, no. 4 (1979): 588–608.

Strain Theory highlights the importance of addressing socio-economic inequalities that drive individuals toward cybercrime.[76] Policy interventions should therefore include programs aimed at improving digital skills, expanding employment opportunities, and reducing economic disparities. In Indonesia, integrating digital literacy and technological training into national development strategies is essential for long-term prevention.

Differential Association Theory emphasizes the need to disrupt the transmission of criminal knowledge within online communities.[77] Law enforcement agencies must enhance their capacity to monitor and infiltrate cybercriminal networks, while educational institutions should promote positive digital values and ethical behavior. Social Control Theory further underscores the importance of strengthening social bonds and normative values to prevent deviant behavior.[78] Public campaigns and educational initiatives should therefore focus on fostering a culture of digital responsibility.

Rational Choice Theory suggests that prevention strategies must increase the perceived risks and reduce the expected benefits of cybercrime.[79] This can be achieved by improving law enforcement efficiency, accelerating judicial processes, and publicizing successful prosecutions to enhance deterrence. In addition, legal reforms must focus on improving clarity and consistency, particularly within the ITE Law, to ensure legal certainty and prevent misuse.[80] International cooperation is also crucial in addressing the transnational nature of cybercrime. Indonesia must strengthen its participation in global initiatives and enhance bilateral and multilateral

[76] Robert K Merton, "Social Structure and Anomie," *American Sociological Review* 3, no. 5 (1938): 672–682.
[77] Edwin H Sutherland, *Principles of Criminology* (4th ed., J.B. Lippincott, 1947).
[78] Travis Hirschi, *Causes of Delinquency* (University of California Press, 1969).
[79] Derek B Cornish and Ronald V Clarke, *The Reasoning Criminal: Rational Choice Perspectives on Offending* (Springer, 1986).
[80] Derek B Cornish and Ronald V Clarke, *The Reasoning Criminal: Rational Choice Perspectives on Offending* (Springer, 1986).

agreements to improve cross-border enforcement.[81] Furthermore, collaboration with the private sector is essential in building a resilient digital ecosystem, as technology companies and financial institutions play a critical role in cybersecurity and incident response.[82]

Finally, improving digital literacy remains a fundamental component of cybercrime prevention. Public awareness programs must be expanded to ensure that individuals understand both the risks and legal implications of digital activities.[83] Without adequate digital literacy, legal and technological measures alone will be insufficient to address the growing threat of cybercrime. In conclusion, the effectiveness of cybercrime regulation in Indonesia depends on the integration of legal frameworks, enforcement mechanisms, and criminological strategies. A holistic approach that combines normative legal reform with preventive and socio-technical interventions is essential for developing a sustainable and adaptive response to cybercrime in the era of technological disruption.

4. Closing

4.1. Conclussion

Cybercrime has emerged as a complex and evolving form of criminality that reflects the intersection between technological advancement, socio-economic conditions, and institutional limitations. This study demonstrates that cybercrime in the era of technological disruption cannot be adequately understood or addressed through a purely legalistic approach. Instead, it requires an integrated perspective that combines legal analysis with criminological insights. From a conceptual standpoint, cybercrime is characterized by its transnational nature, anonymity, and capacity for large-scale impact, distinguishing it from conventional forms of crime.

[81] UNODC, *Cybercrime Strategy Report* (2020).
[82] World Economic Forum, *Global Cybersecurity Outlook* (2023).
[83] Kementerian Komunikasi dan Informatika, *Status Literasi Digital Indonesia* (2022).

Criminological theories including Routine Activity Theory, Strain Theory, Differential Association Theory, Social Control Theory, and Rational Choice Theory provide a comprehensive framework for understanding the motivations and behaviors of cybercriminals. These theories reveal that cybercrime is driven by the convergence of opportunity, socio-economic pressures, weak social control, and rational decision-making processes in digital environments. In the Indonesian context, although a legal framework has been established through the ITE Law, the Personal Data Protection Law, and PP PSTE, its effectiveness remains limited. The study finds that legal provisions often suffer from ambiguity, particularly within the ITE Law, while enforcement mechanisms face significant challenges, including limited human resources, inadequate technological infrastructure, complexities in digital evidence, and jurisdictional constraints. These weaknesses contribute to the perception that cybercrime is a low-risk and high-reward activity, thereby sustaining its growth. Furthermore, the findings indicate that cybercrime in Indonesia is not solely a legal issue but also a structural and social problem. Factors such as economic inequality, low digital literacy, technological accessibility, and weak institutional coordination play a significant role in facilitating cybercriminal activities. As a result, law enforcement strategies that focus exclusively on punitive measures are insufficient to address the root causes of cybercrime. This study concludes that the effectiveness of cybercrime prevention and law enforcement in Indonesia depends on the integration of legal, criminological, and technological approaches. A holistic strategy that combines regulatory reform, institutional strengthening, technological advancement, and socio-cultural intervention is essential to create a resilient digital security system. Without such integration, efforts to combat cybercrime will remain reactive and fragmented.

4.2. Suggestion

Based on the findings of this study, several strategic recommendations are proposed to enhance the effectiveness of cybercrime prevention and law enforcement in Indonesia. First, legal reform is necessary to improve the clarity, consistency, and adaptability of existing regulations. The ITE Law, in particular, should be refined to eliminate ambiguous provisions and ensure alignment with the principles of legal certainty and proportionality. Additionally, the implementation of the Personal Data Protection Law must be strengthened through the establishment of an independent supervisory authority and clear enforcement mechanisms. Second, institutional capacity building should be prioritized. Law enforcement agencies require continuous training in digital forensics, cybersecurity, and data analysis, supported by adequate technological infrastructure. The development of specialized cyber units across all regions is essential to ensure equitable law enforcement capabilities. Third, the government should enhance digital literacy programs as a preventive measure. Public education initiatives must focus not only on technical skills but also on legal awareness and ethical responsibility in digital environments. Improving digital literacy will reduce both victimization and participation in cybercrime. Fourth, stronger coordination among institutions is required. Effective cybercrime prevention demands collaboration between law enforcement agencies, regulatory bodies, financial institutions, and private sector actors. Establishing integrated coordination mechanisms will improve response efficiency and reduce institutional fragmentation. Fifth, Indonesia must strengthen international cooperation to address the transnational nature of cybercrime. This includes expanding bilateral and multilateral agreements, participating actively in global cybercrime initiatives, and harmonizing national laws with international standards. Finally, future research should focus on empirical studies of cybercrime in Indonesia, particularly in relation to behavioral patterns, victimology, and the effectiveness of policy interventions. Such research will provide a stronger evidence base for developing adaptive and

data-driven strategies in combating cybercrime. In conclusion, addressing cybercrime requires a paradigm shift from reactive enforcement to proactive and preventive governance. By integrating legal, criminological, and technological approaches, Indonesia can develop a more effective, sustainable, and resilient response to cybercrime in the digital era.

REFERENCES

Accenture. *Cost of Cybercrime Study*. 2023.

Amnesty International. *Pasal-pasal Karet dalam UU ITE dan Dampaknya terhadap Kebebasan Berekspresi di Indonesia*. 2020.

Badan Siber dan Sandi Negara (BSSN). *Laporan Statistik Serangan Siber Nasional Tahun 2023*. 2023.

Badan Siber dan Sandi Negara (BSSN). *Strategi Keamanan Siber Nasional*. 2022.

Badan Siber dan Sandi Negara (BSSN). *Laporan Tahunan Keamanan Siber*. 2023.

Bappenas. *Laporan Pembangunan Digital Indonesia*. 2022.

Barda Nawawi Arief. *Kebijakan Hukum Pidana dalam Penanggulangan Cyber Crime*. Citra Aditya Bakti, 2018.

Brenner, Susan W. *Cybercrime: Criminal Threats from Cyberspace*. Praeger, 2010.

Cohen, Lawrence E., and Marcus Felson. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44, no. 4 (1979): 588–608. https://doi.org/10.2307/2094589.

Cornish, Derek B., and Ronald V. Clarke. *The Reasoning Criminal: Rational Choice Perspectives on Offending*. Springer, 1986. https://doi.org/10.1007/978-1-4613-8625-5.

ENISA. *Threat Landscape Report*. 2023.

ENISA. *Cybersecurity Culture Guidelines*. 2022.

Europol. *Internet Organised Crime Threat Assessment (IOCTA)*. 2022.

Hirschi, Travis. *Causes of Delinquency*. University of California Press, 1969. https://doi.org/10.1525/9780520340756.

Institute for Criminal Justice Reform (ICJR). *Reformulasi UU ITE*. 2021.

INTERPOL. *Global Cybercrime Report*. 2023.

Kementerian Komunikasi dan Informatika Republik Indonesia. *Status Literasi Digital Indonesia*. 2022.

Kementerian Komunikasi dan Informatika Republik Indonesia. *Pedoman Perlindungan Data Pribadi*. 2023.

Kepolisian Republik Indonesia. *Laporan Kinerja Dittipidsiber*. 2023.

Marzuki, Peter Mahmud. *Penelitian Hukum*. 17th ed. Jakarta: Prenada Media, 2022.

Merton, Robert K. "Social Structure and Anomie." *American Sociological Review* 3, no. 5 (1938): 672–682. https://doi.org/10.2307/2084686

Nugroho, R., and I. M. Putri. "Strategi Penegakan Hukum terhadap Kejahatan Siber di Indonesia." *Jurnal Hukum dan Pembangunan* 51, no. 2 (2021): 273–290. https://doi.org/10.21143/jhp.vol51.no2.2892

OECD. *Digital Security Risk Management*. 2020. https://doi.org/10.1787/8b92f4fe-en.

OECD. *Digital Security Behaviour Report*. 2021. https://doi.org/10.1787/9c45c9b0-en.

Otoritas Jasa Keuangan (OJK). *Laporan Penanganan Pinjaman Online Ilegal*. 2023.

Otoritas Jasa Keuangan (OJK). *Laporan Sektor Jasa Keuangan Digital*. 2023.

Sutherland, Edwin H. *Principles of Criminology*. 4th ed. J.B. Lippincott, 1947.

UNODC. *Comprehensive Study on Cybercrime*. 2013.

UNODC. *Cybercrime Strategy Report*. 2020.

World Bank. *Digital Development Report*. 2021. https://doi.org/10.1596/978-1-4648-0671-1.

World Economic Forum. *Global Cybersecurity Outlook*. 2023. https://doi.org/10.2139/ssrn.4332248.

Wall, David S. *Cybercrime and Society*. 2nd ed. Sage, 2017. https://doi.org/10.4135/9781473906396.

Holt, Thomas J. *Cybercrime and Digital Deviance*. Routledge, 2016. https://doi.org/10.4324/9781315670256.

Yar, Majid. *Cybercrime and Society*. Sage, 2017. https://doi.org/10.4135/9781529715229.

Legislation

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan UU ITE.

Undang-Undang Nomor 1 Tahun 2024.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.