Universitas Internasional Batam
Fakultas Hukum
Jl. Gadjah Mada, Batam, 29442, Indonesia
Phone : (0778) 743 7111 Ext, 140.
Email: admin_jlpt@gmail.com

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 10, No. 2-December 2025

RECONSTRUCTION OF THE INFORMATION TECHNOLOGY-BASED CYBERCRIME PREVENTION MODEL IN THE NATIONAL CYBER LAW SYSTEM

Erlan Bachtiar[1]*, Ninin Ernawati[2]**
Universitas Nusa Mandiri*, Universitas Katolik Indonesia Atma Jaya**

Abstract

The increasingly complex development of information technology has increased the frequency and variety of cybercrime in Indonesia. Although the national legal framework, particularly Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), has provided a legal basis for combating cybercrime, effective prevention still faces challenges. These challenges include a lack of synchronized norms, limited early detection mechanisms, low system interoperability, and slow policy updates compared to the rapid evolution of cybercrime methods. This study aims to analyze the weaknesses of the current prevention model in the national cyber law system and formulate a reconstruction of a more adaptive, responsive, and technology-based cybercrime prevention model oriented toward strengthening cyber resilience. Using a juridical-normative approach, this study examines laws and regulations, court decisions, and international information security standards. The analysis results indicate the need for an integrated prevention model that includes: an AI-powered threat intelligence-based early detection system and cross-sectoral regulatory harmonization. This model reconstruction is expected to serve as a foundation for updating national cyber law policies to be more effective in addressing the dynamics of cyber threats in the digital era.

Keywords: *Cybercrime, Cybersecurity, Information Technology-Based Prevention, Model Reconstruction, Indonesian Cyber Law.*

A. Background

The development of information technology in Indonesia has brought significant transformations to various sectors of life, including the economy, government, education, and public services.[3] However, this digital progress has been accompanied by a growing risk of cybercrime, which is increasingly varied, complex, and difficult to detect.[4] This phenomenon is evident in the increasing trend of cyberattacks targeting personal data, government systems, electronic transactions, and even vital national infrastructure. Cybercrime not only causes economic losses but also threatens national security, public trust, and the stability of a country's information systems.[5]

Real-life examples of cybercrime in Indonesia that demonstrate increasingly varied and complex crime patterns include the ransomware attack on the Temporary National Data Center (PDNS) on June 20, 2024, which paralyzed various government services

[1]* Corresponding Author: erlan.bachtiar@gmail.com
[2]** ninin.ernawati@atmajaya.ac.id

[3] Herie Saksono Aminah, Sitti, "Digital Transformation of the Government: A Case Study in Indonesia," in *Jurnal Komunikasi: Malaysian Journal of Communication*, vol. 37, 2021, 272–88, https://doi.org/https://doi.org/10.1007/978-3-031-36001-5_37.

[4] Hamed Taherdoost, "Insights into Cybercrime Detection and Response: A Review of Time Factor," *Information* 15, no. 5 (2024): 273, https://doi.org/https://doi.org/10.3390/info15050273.

[5] Howard Rush Kraemer-Mbula, Erika, Puay Tang, "The Cybercrime Ecosystem: Online Innovation in the Shadows?," *Technological Forecasting and Social Change* 80, no. 3 (2013): 541–55, https://doi.org/https://doi.org/10.1016/j.techfore.2012.07.002.

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 10, No. 2-December 2025

(including immigration services) and was accompanied by a ransom demand of approximately US$8 million. The government stated that it would not pay the ransom and implemented a phased recovery. Another major case was the disruption of Bank Syariah Indonesia (BSI) services in May 2023, which was later linked to LockBit ransomware, with reports of data theft and digital extortion. In the realm of data leaks and trading, Indonesia was also shaken by the alleged leak of BPJS Kesehatan participant data, which was widely discussed in May 2021, with the issue of large amounts of data allegedly being traded on online hacker forums. Meanwhile, AI/deepfake-based methods have also entered the realm of public fraud: in January 2025, the police uncovered a fraud using deepfake videos that impersonated President Prabowo Subianto to deceive victims (the "aid program" method), and is said to have deceived many people since 2024. This condition demands that the state have an adaptive and technology-oriented prevention model.

Indonesia already has a legal framework governing the digital space through Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law)[6] and its amendment in Law Number 19 of 2016, which serves as the legal basis for regulating unlawful acts in cyberspace.[7] Furthermore, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE) provides guidelines for the implementation of electronic systems, while Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) strengthens the security of individual data as a fundamental component of cybersecurity.[8] The presence of technical regulations from the National Cyber and Crypto Agency (BSSN), such as information security standards, cyber incident management, and risk management guidelines, further complements the national legal framework.

However, these regulations are not yet fully capable of addressing the rapidly evolving dynamics of modern cyberattacks—from phishing and ransomware to data breaches and AI-based attacks. The main challenges to cybercrime prevention in Indonesia lie in weak policy integration, suboptimal early detection systems, limited inter-agency coordination, and limited cyber threat intelligence capabilities. Furthermore, the prevailing prevention model tends to be reactive and focuses more on legal enforcement than proactive, technology-based prevention.

Globally, several countries have adopted a cyber resilience approach through the integration of artificial intelligence, machine learning, predictive analytics, and cross-sector policy harmonization. Meanwhile, Indonesia needs to reconstruct its cybercrime prevention model, combining legal instruments with modern information technology approaches, so that the national cyber law system can be more adaptive, comprehensive, and effective in addressing digital threats.

Based on these conditions, in-depth research is needed to analyze the weaknesses of existing prevention models and formulate ideas for reconstructing a technology-based

---

6 Muhammad Ishar Helmi Kharlie, Ahmad Tholabi, "The Role of the Law on Electronic Information and Transactions in Overcoming Challenges of Democracy in Indonesia," *International Journal of Advanced Science and Technology* 28, no. 20 (2019): 1178–84, https://doi.org/https://fathudin85.wordpress.com/wp-content/uploads/2020/02/3505-article-text-5555-1-10-20200120.pdf.

7 Thomas Paterson, "Indonesian Cyberspace Expansion: A Double-Edged Sword," *Journal of Cyber Policy* 4, no. 2 (2019): 216–34, https://doi.org/https://doi.org/10.1080/23738871.2019.1627476.

8 Haekal Al Asyari, "Between Freedom And Protection: A Critical Review Of Indonesia'S Cyberspace Law," *Prophetic Law Review* 5, no. 1 (2023): 79–103, https://doi.org/https://doi.org/10.20885/PLR.vol5.iss1.art5.

cybercrime prevention model. This research is crucial not only for strengthening the national cyber law system but also for supporting the government's efforts to improve digital security, protect public data, and create a safe cyberspace in accordance with the principles of good digital governance in the era of digital transformation.

Various previous studies have shown that cybercrime prevention in Indonesia still faces serious challenges, both in terms of regulation and technological readiness. Previous research has highlighted that Indonesia's legal response to cybercrime is entering a new phase following the enactment of the 2023 Criminal Code (KUHP), which introduces significant changes to the national legal system, particularly in the cybercrime domain. (Suseno et al., 2024) argue that the updated framework seeks to strengthen Indonesia's criminal law in addressing the proliferation of digital crimes by incorporating and refining several provisions previously regulated under the ITE regime. Using a normative legal approach and examining key legislation—especially Law No. 1 of 2024 amending Law No. 11 of 2008 on Electronic Information and Transactions and Law No. 1 of 2023 on the Criminal Code—the study notes that the amendments cover issues such as defamation and insults, blasphemy, privacy violations, threats and intimidation, moral offences, pornography, and other related cybercrimes. Importantly, the research emphasizes that these reforms are intended to respond to the challenges of the digital era and reduce normative overlaps or conflicts between the ITE Law and the new Criminal Code. The study concludes that cybercrime in Indonesia is likely to continue increasing rapidly, with the growing use of Artificial Intelligence further intensifying the scale and complexity of threats.

On the other hand, (Astuti, 2021) found that an approach that overemphasizes digital literacy has not been effective in reducing cybercrime rates. Criminals are now using increasingly complex techniques, including the use of AI for phishing and social engineering, so educational campaigns are no longer sufficient as a sole strategy. This aligns with the findings of (Effendi & Kurniawan, 2022), who developed an integrated cyber-monitoring model based on machine learning. The model achieved over 90% detection accuracy, but they noted the lack of legal legitimacy governing the use of algorithms, data processing, and secure response mechanisms. This regulatory vacuum creates the potential for privacy violations and legal uncertainty.

Another study by (Putra, 2023) highlighted that Indonesia's cyber legal system has not been harmonized with global standards such as the Budapest Convention, particularly regarding early warning systems and the exchange of cyber intelligence data. This disharmony has left Indonesia lagging behind in developing an information technology-based prevention system. Overall, previous studies have shown that although the use of information technology has been shown to improve detection and prevention capabilities, there is no model that comprehensively integrates technological and legal aspects into a unified cybercrime prevention framework.

Various previous studies have revealed significant gaps in cybercrime prevention efforts in Indonesia. To date, there is no comprehensive prevention model that integrates information technology with the national legal framework. Previous studies tend to be fragmented: some focus solely on technological aspects such as artificial intelligence, monitoring systems, and cyberthreat intelligence, while others focus on regulations without establishing a link with technological innovation. Furthermore, there is still a lack of operational regulatory standards that clearly govern the use of algorithms, digital data processing, and early detection mechanisms in the context of cybercrime prevention.

This legal vacuum means that the application of modern technology has the potential to raise privacy issues and uncertainty about law enforcement.

Furthermore, Indonesia's cyber law system remains reactive—more focused on regulating after a crime has occurred than providing a measurable, technology-based preventive framework. [9] The lack of alignment between the needs of modern cybersecurity technology and national and international legal instruments is also a significant obstacle; although several studies have highlighted this gap, none have offered an integrative model to address it. Therefore, this study aims to fill this gap by reconstructing a cybercrime prevention model that integrates information technology and the national cyber law system. The expected outcome is a more modern, preventative approach that can respond to evolving cyber threats in a comprehensive and sustainable manner.

B. Identified Problems

1. What are the normative and technical weaknesses that still hamper cybercrime prevention in Indonesia?
2. How can we formulate a more comprehensive, responsive, and adaptive reconstruction of a technology-based cybercrime prevention model to strengthen the national cyber law system?

C. Research Methods

This research employs a normative juridical research method, [10] namely legal research that positions law as a norm or principle applicable in society. This approach aims to examine and analyze positive legal provisions governing cybercrime, electronic evidence, and prevention and mitigation mechanisms within the framework of national cyber resilience. Normative juridical research was chosen because the focus of the study is directed at written legal norms, legal principles, and relevant doctrines, rather than on legal behavior in empirical practice.

The approach used in this research includes a statutory approach, [11] examining various laws and regulations related to cybercrime and electronic evidence, such as the Criminal Procedure Code (KUHAP), the Electronic Information and Transactions Law (UU), the Personal Data Protection Law (UU), and other implementing regulations. Furthermore, a conceptual approach is used to understand legal concepts developed in the literature, including cybercrime, electronic evidence, criminal evidence systems, and cyber resilience. To some extent, this research also uses a comparative approach by referring to international principles and practices related to cybersecurity regulations and incident reporting as material to enrich the analysis.

The legal sources used in this research consist of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials include laws and

[9] F. Satoto, E., & Santiago, "Reconstruction of Indonesia's Cyber Law System for Adaptive and Integrated Digital Crime Prevention in the Era of Technological Disruption," *Greenation International Journal of Law and Social Sciences* 3, no. 2 (2025): 309–17, https://doi.org/https://doi.org/10.38035/gijlss.v3i2.425.

[10] M. H. M. Hamzani, A. I., Widyastuti, T. V., Khasanah, N., & Rusli, "Legal Research Method: Theoretical and Implementative Review," *International Journal of Membrane Science and Technology* 10, no. 2 (2023): 3610–19.

[11] T. A. S. Negara, "Normative Legal Research in Indonesia: Its Originis and Approaches," *Audito Comparative Law Journal (ACLJ)* 4, no. 1 (2023): 1–9, https://doi.org/https://doi.org/10.22219/aclj.v4i1.24855.

regulations, court decisions (if relevant), and official state documents. Secondary legal materials include legal textbooks, scientific journals, research results, and expert opinions related to cyber law and criminal evidence. Tertiary legal materials, such as legal dictionaries and encyclopedias, are used as supporting sources to clarify certain terms and concepts.

The legal materials were collected through library research, which involved searching and inventorying relevant legal materials from both print and digital sources. The collected legal materials were then analyzed using qualitative analysis, interpreting legal norms systematically, consistently, and logically, and relating them to the legal issues under study. The results of the analysis were then presented descriptively and analytically, describing applicable legal provisions while providing legal arguments to address the research problems and drawing normative conclusions.

D. Research Findings and 1Discussion

Reconstructing a More Comprehensive, Responsive, and Adaptive Information Technology-Based Cybercrime Prevention Model

Reconstructing the cybercrime prevention model requires a multidimensional approach that integrates legal, technological, and institutional aspects. Conceptually, the new model must adopt the principles of preventive cyber law, a legal paradigm that operates before a crime occurs through the use of information technology. This model can be built by positioning technology as a primary prevention tool, for example through AI-based threat detection, machine learning to interpret attack patterns, national cyberthreat intelligence, and the integration of a cyber incident data center. This system enables the government to conduct early detection, provide rapid warnings, and mitigate vulnerabilities before they are exploited by perpetrators.

AI-based threat detection is a cybersecurity approach that uses artificial intelligence[12]—specifically machine learning, deep learning, and behavioral analytics—to identify, analyze, and respond to threats automatically and in real time.[13] These systems process large volumes of data (network logs, endpoint activity, cloud telemetry, etc.) to find patterns, anomalies, or indicators of compromise, enabling them to detect both known threats and new/zero-day attacks that lack signatures. With the ability to learn from data and adapt to changing attack tactics, AI-based threat detection is a key component of modern cybercrime prevention models at both the organizational and national levels.

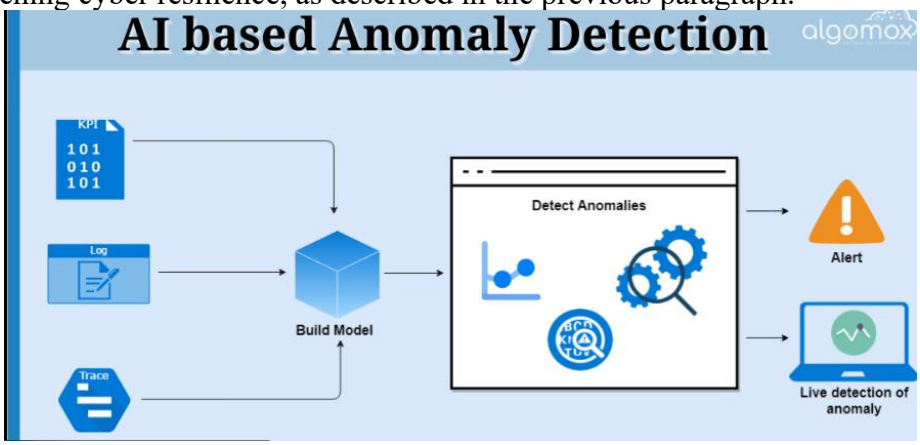
In practice, the implementation of AI-based threat detection enables security systems to proactively detect suspicious activity before it develops into a major incident, for example through user and entity behavior analytics (UEBA) monitoring to identify account misuse, unusual access, or privilege escalation. This technology is also capable of automating incident response, such as isolating infected devices, blocking malicious connections, or dynamically adjusting security policies, thereby reducing reliance on

[12] S. Ramesh, S. K. A., & Kiran, "AI-Enhanced Cyber Threat Detection," *International Journal of Computer Trends and Technology (IJCTT)* 72, no. 6 (2024): 64–71, https://doi.org/https://doi.org/10.14445/22312803/IJCTT-V72I6P109.

[13] Enjina Sivakumar, Janaki and Salman, Nawras Rafid and Salman, Farah Rafid and Salimova, Husniya Rustamovna and Ghimire, "AI-Driven Cyber Threat Detection : Enhancing Security through Intelligent Engineering Systems," *Journal of Information Systems Engineering and Management* 10, no. 19 (2025): 790–98, https://doi.org/https://doi.org/10.52783/jisem.v10i19s.3116.

manual intervention and accelerating response times. In the Indonesian context, the use of AI-based threat detection is relevant for protecting critical sectors such as digital public services, banking, and healthcare infrastructure, which are prime targets of cyberattacks, while also supporting the strengthening of national cyber resilience through early warning systems, cross-agency collaboration, and data-driven decision-making.

The following illustrates how AI-based threat detection works in the modern cybersecurity ecosystem. The visual flow shows how various data sources—such as network logs, user activity, endpoints, and cloud services—are centrally collected and analyzed by an artificial intelligence-based system. Through machine learning algorithms and behavioral analytics, the system learns normal activity patterns and then compares them with ongoing activity to identify anomalies or indications of cyberattacks. The results of this analysis are displayed in a real-time Security Operations Center (SOC) dashboard, allowing for early detection and automated action, such as blocking access, isolating systems, or issuing early warnings to security analysts. This image thus clarifies how AI-based threat detection supports proactive detection, rapid response, and strengthening cyber resilience, as described in the previous paragraph.



Source: Algomox.com

Strengthening AI-based threat detection at a later stage can be directed at three complementary pillars: machine learning to read attack patterns, national cyber threat intelligence (CTI), and integration of cyber incident data centers. First, the use of machine learning enables organizations and regulators to analyze attack traces over time—for example, scanning patterns, repeated login attempts, lateral movement, and escalation of access rights—so that the system can distinguish normal activity from anomalies with greater precision and predict increased risk to specific assets. Second, national CTI serves as a mechanism for structured threat knowledge sharing across sectors (government, financial, healthcare, telecommunications), including indicators of compromise (IOCs), perpetrator tactics-techniques-procedures (TTPs), vulnerability trends, and early warnings. Thus, detection in one institution can immediately become collective learning for other institutions. Third, integration of cyber incident data centers strengthens response coordination through the consolidation of incident reports, correlation across telemetry sources, and impact mapping, allowing for faster and evidence-based forensic investigations, service restoration, and mitigation prioritization. If these three components work in an integrated manner, cybercrime prevention will not

only be reactive at the organizational level, but will develop into a systemic cyber resilience capacity at the national level.

The use of machine learning to read attack patterns means that threat detection no longer relies on static signatures, but rather on learning from historical patterns and actual behavior. The system collects attack traces over time—for example, repeated scans from a specific IP, spikes in login attempts (brute force/credential stuffing), indications of lateral movement between hosts after a single account/machine compromise, and privilege escalation patterns such as sudden role changes or unusual access to sensitive services. From this data, the model builds a baseline of normal activity for each asset or user (e.g., access hours, location, traffic volume, commonly used applications), then compares it to ongoing activity to identify meaningful anomalies, not just outliers.

In an operational context, ML helps with two important things. First, correlating sequences of events: a single event might seem normal (e.g., a failed login), but if it's followed by scanning, access to a file server, and then a large data transfer, the model can raise the risk score because the pattern resembles an attack kill chain. Second, predicting increased risk for a specific asset: if the model sees a recurring trend (e.g., asset A is consistently targeted for scanning, or a particular account frequently experiences login attempts from multiple locations), the system can deem that asset "high risk" and recommend countermeasures such as mandatory MFA, access restrictions, network isolation, or increased monitoring. In this way, machine learning not only accelerates detection but also strengthens data-driven prevention, allowing organizations to intervene before attacks escalate into major incidents.

National Cyber Threat Intelligence (CTI) is essentially a collective mechanism for collecting, verifying, and then sharing cyber threat information in a structured manner across sectors—for example, government, finance, healthcare, and telecommunications—so that all parties have a “common threat picture” and can respond more quickly. The information shared includes not only indicators of compromise (IOCs) such as IP addresses, malicious domains, malware hashes, phishing URL patterns, or other forensic artifacts, but also actor tactics–techniques–procedures (TTPs) that explain how attacks work (e.g., credential stuffing, admin account abuse, lateral movement, or data exfiltration). Furthermore, national CTI typically includes vulnerability trends (e.g., actively exploited CVEs), context of vulnerable targets, and early warnings of ongoing attack campaigns.

Its primary value lies in the “collective learning” effect: when one institution detects a particular attack pattern, it can quickly translate that finding into intelligence that other institutions can use to strengthen their defenses—for example, blocking IOCs, adding detection rules in SIEM/EDR, applying priority patches, or closing configuration gaps before an attack occurs. In this way, national CTI eliminates the “every agency fending for itself” situation and replaces it with a unified, data-driven response, accelerating detection and mitigation times, especially in the case of massive, fast-moving attacks targeting multiple sectors simultaneously.

The integration of a cyber incident data center strengthens response coordination because all incident reports from multiple organizations can be compiled into a single, unified repository, eliminating the need for authorities and response teams to work with fragmented information. This consolidation allows incident data—such as timelines, indicators of compromise, critical logs, and triage results—to be correlated with cross-source telemetry (SIEM, EDR, firewall, IDS/IPS, cloud logs, and identity) to identify

common attack patterns, attack chains, and possible linkages between events in different sectors. The data center also enables more objective impact mapping, such as which services were disrupted, which critical assets were affected, the distribution of victims, and the potential for escalation. This allows for more focused forensic investigations, prioritized service restoration, and evidence-based mitigation decisions, rather than guesswork. If the integration of this incident data center works in harmony with the ability of machine learning to read attack patterns and the national CTI mechanism to share indicators and TTPs quickly, then cybercrime prevention will no longer stop at reactive responses at the organizational level, but will instead increase to systemic national cyber resilience—where early detection, collective learning, and cross-sector coordination become a continuous cycle.

In conclusion, strengthening modern cybercrime prevention requires an integrated approach, no longer relying on incidental responses in individual organizations. Machine learning plays a role in dynamically reading attack traces and patterns, enabling more precise anomaly detection and risk prediction. National Cyber Threat Intelligence (CTI) then ensures that threat findings from a single institution are quickly shared across sectors in the form of compromise indicators, perpetrator TTPs, vulnerability trends, and early warnings, enabling collective learning. Furthermore, the integration of cyber incident data centers strengthens coordination through report consolidation, telemetry correlation, and impact mapping, enabling faster and evidence-based forensic investigations, service restoration, and mitigation priorities. When these three components operate in an integrated manner, the cybersecurity system evolves from a reactive model to a systemic, adaptive, and sustainable national cyber resilience.

Legal Issues in Tackling Cyber Crime in Indonesia

Cybercrime is a relatively new form of crime and is generally committed by perpetrators with knowledge and skills in computers and information technology.[14] Its impacts occur not only in the digital space but can also cause real harm outside of cyberspace [15]. The internet's transcendent nature makes cyberspace activities difficult to detect using conventional methods.[16] Technological developments have also transformed the function of computers, from primarily as data processing, storage, and management tools, into tools for committing "old" crimes in more modern forms and modes.[17] Therefore, when computer and cybercrime cases are analyzed using conventional criminal law criteria, their complexity is not simple. Within a conventional legal framework, acts such as fraud, deception, theft, and vandalism are generally committed directly by the perpetrator; however, when using cyber means, the range of acts becomes more diverse and multi-layered.

---

[14] V. N. Kirillova, E. A., Bogdan, V. V., Golovatskaya, M. V., Melnichenko, T. A., & Ognev, "Legal Significance of Electronic Messages and Documents," *Journal of Advanced Research in Law and Economics* 9, no. 3 (2018): 997–1003, https://doi.org/https://www.ceeol.com/search/article-detail?id=735202.

[15] M Lagazio, M., Sherif, N., & Cushman, "A Multi-Level Approach to Understanding the Impact of Cyber Crime on the Financial Sector," *Computers & Security* 45 (2014): 58–74, https://doi.org/https://doi.org/10.1016/j.cose.2014.05.006.

[16] D. Hunter, "Cyberspace as Place and the Tragedy of the Digital Anticommons," in *Law and Society Approaches to Cyberspace*, 2017, 59–139, https://doi.org/https://www.taylorfrancis.com/chapters/edit/10.4324/9781351154161-3/cyberspace-place-tragedy-digital-anticommons-dan-hunter.

[17] B. D. Thomas, D., & Loader, "Introduction: Cybercrime: Law Enforcement, Security and Surveillance in the Information Age," in *Cybercrime* (Routledge, 2013), 1–14.

Soepraptomo explains that computer and cybercrime can appear in several main forms. First, computer fraud, which includes, among other things, entering unauthorized instructions into the system for personal gain (e.g., unauthorized transfers), manipulating input data to benefit oneself or others (e.g., increasing salary data beyond what is expected), damaging or obscuring output to hide information, and using computers as a means of solving or obtaining information that is then used to commit crimes or change programs. This type of fraud can also be used to avoid certain obligations or obtain something that is not rightfully owned through computers. Besides being carried out by a single perpetrator, computer fraud can take the form of a conspiracy, that is, carried out together by several people.

In this context, theft is also understood as the intentional and unlawful taking of another person's rights or property for one's own use. Second, the crime of embezzlement and falsification of information through computers that harms another party and benefits the perpetrator. Third, hacking, namely access to a computer system without permission or unlawfully to penetrate security and threaten certain interests, including hacking online systems that utilize communication networks. Fourth, destruction of a computer system, whether in the form of data destruction, deletion of code, addition or change of programs/information/media that results in system damage and loss, including the spread of viruses and extortion using computers or telecommunications. Fifth, crimes related to intellectual property rights such as copyright and patent infringement through piracy, for example producing counterfeit goods to gain profit from trade.

Meanwhile, Asril Sitompul offers a more concise classification by grouping cybercrime into several categories: data-related crimes (e.g., termination or disruption of data transfer), network-related crimes such as wiretapping and sabotage, internet-related crimes such as hacking and spreading viruses, and crimes related to the use of computers to support crimes in cyberspace, including data falsification for profit or to be treated as genuine data. In addition, he also includes capital market-related crimes and content-related crimes, such as pornography, insults, defamation, and various other unlawful acts.

In the Indonesian criminal law system, cybercrime is generally positioned as a special crime.[18] Although its elements can often be matched with a number of provisions in the Criminal Code, this crime is committed through newer modes and means (new design) so that it requires separate regulations. Indonesia already has Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) which was passed in March 2008 and then amended by Law No. 19 of 2016 which was promulgated on November 25, 2016. The presence of the ITE Law adds criminal norms, both from a material and formal perspective, which in principle can be applied as special provisions in accordance with the principles in Article 103 of the Criminal Code and Article 284 paragraph (2) of the Criminal Procedure Code.

If examined closely, the ITE Law is a complex regulation because it contains civil, criminal, and administrative dimensions simultaneously. In the criminal realm, especially in Chapter VII (around Articles 27–37), the ITE Law formulates a number of prohibited acts which include: distribution, transmission, or making accessible electronic information/documents containing violations of morality, gambling, insults or defamation, as well as blackmail or threats; dissemination of false/misleading news that

[18] E. C. Viano, "Cybercrime: Definition, Typology, and Criminalization," in *Cybercrime, Organized Crime, and Societal Responses: International Approaches*, 2016, 3–22, https://doi.org/https://doi.org/10.1007/978-3-319-44501-4_1.

is detrimental to consumers in electronic transactions and dissemination of information that causes hatred or hostility based on ethnicity, religion, race, and intergroup relations (SARA); sending electronic information containing threats of violence or intimidation aimed at individuals; unauthorized access to computers/electronic systems, including access to obtain electronic information and access by breaking through or breaking security systems; interception or tapping of electronic information/documents or the transmission of information that is not public, whether resulting in changes or resulting in the removal or termination; actions against data such as changing, adding, reducing, transmitting, damaging, removing, moving, or hiding electronic information/documents belonging to other parties or the public, including the transfer of data to the system of an unauthorized party; actions that disrupt electronic systems so that they do not function properly; production, sale, procurement, import, distribution, provision, or ownership of hardware/software or passwords/access codes designed to facilitate such prohibited acts; manipulation or engineering of electronic information/documents to appear authentic; acts that cause harm to others; and the affirmation of extraterritorial scope, namely the prohibition of carrying out such acts from outside the territory of Indonesia as long as they attack electronic systems within Indonesian jurisdiction.

In resolving the legal issue of cyber crime, the judge does not have to find all the evidence1 that has been determined, but based on Article 183 of the Criminal Procedure Code, a criminal verdict can be issued by the judge with at least two valid pieces of evidence and he truly believes that the crime has indeed occurred and the defendant is the one who committed the crime. R. Subekti calls it a "negative system according to law".[19]

The negative evidentiary system according to the law essentially contains two main points. First, to declare a defendant guilty, the minimum limit of evidence as determined by law must be met.[20] Second, even if the evidence presented has exceeded the minimum limit, a guilty verdict cannot be rendered if the judge has not yet reached a conviction regarding the defendant's guilt;[21] in such a condition the judge is not permitted to blame or sentence the defendant. In line with this, Yahya Harahap explains that the negative evidentiary system according to the law (negatief wettelijk stelsel) is a form of middle ground between the positive evidentiary system according to the law and the evidentiary system that relies entirely on the judge's conviction (conviction intime).

In addition to the evidence specified in Article 184 paragraph (1) of the Criminal Procedure Code, the development of information technology has given rise to new forms of evidence, namely electronic evidence in the form of electronic information and electronic documents, as an extension of the previously known evidentiary regime. Article 44 of the ITE Law emphasizes that in addition to evidence according to the Criminal Procedure Code, the evidentiary system also recognizes evidence in the form of electronic information and/or electronic documents as formulated in Article 1 number

[19] S. Sunaryo, "The Meaning of'against Justice'in Judicial Decisions of Criminal Cases in Indonesia," *International Journal of Public Law and Policy* 10, no. 4 (2024): 359–82, https://doi.org/https://doi.org/10.1504/IJPLAP.2024.141710.

[20] W. Sulistyani, "The Admissibility of Scientific Expert Evidence under Indonesian Criminal Justice System," *Sriwijaya Law Review* 3, no. 2 (20919): 152–61, https://doi.org/https://doi.org/10.28946/slrev.Vol3.Iss2.215.pp152-161.

[21] S. Butt, "Indonesia's Criminal Justice System on Trial: The Jessica Wongso Case," *New Criminal Law Review* 24, no. 1 (2021): 3–58, https://doi.org/https://doi.org/10.1525/nclr.2021.24.1.3.

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 10, No. 2-December 2025

(1) and number (4) and Article 5 paragraph (1), paragraph (2), and paragraph (3) of the ITE Law. Furthermore, based on Article 1 number (1) of the ITE Law, electronic information is understood as one electronic data or a collection of electronic data, the scope of which includes—without being limited to—writing, sound, images, maps, designs, photos, electronic data interchange (EDI), electronic mail (email), telegrams, telex, telecopy, or similar forms, including letters, signs, numbers, access codes, symbols, or perforations that have been processed so that they have meaning or can be understood by parties who are competent to interpret them.

According to Article 1 number (4) of the ITE Law, electronic documents are defined as any electronic information created, forwarded, sent, received, or stored in various forms—whether analog, digital, electromagnetic, optical,[22] or similar forms—that can be seen, displayed, and/or heard via a computer or electronic system. The scope includes, but is not limited to, writing, sound, images, maps, designs, photographs or similar forms, as well as letters, signs, numbers, access codes, symbols, or perforations that have been processed so that they have meaning and can be understood by parties who are able to understand them. Furthermore, Article 5 of the ITE Law emphasizes the position of electronic evidence as valid evidence by stating that electronic information and/or electronic documents and their printouts are valid legal evidence, and are also seen as an expansion of the evidence recognized under the applicable procedural law in Indonesia. The validity of electronic information and/or electronic documents also requires the use of an electronic system that meets the provisions as stipulated in the ITE Law. In addition, recognition of electronic media-based evidence actually emerged earlier through Law No. 8 of 1997 concerning Company Documents, which in Article 15 paragraph (1) confirms that company documents contained in microfilm or other media, including printed copies, can be used as valid evidence.

The expansion of conventional evidence as regulated in Article 184 paragraph (1) of the Criminal Procedure Code has opened up space for the introduction of evidence that is more progressive and responsive to current developments, including the recognition of electronic data or electronic evidence. However, in the practice of providing evidence, electronic evidence raises a number of problems. First, regarding the locus delicti, investigators often face difficulties in determining the location of the crime accurately because the perpetrator can delete or change digital traces, even arrange the location (for example through configuration engineering or certain services) so that it appears different from the actual location.

Second, the issue of tempus delicti also presents a challenge, as perpetrators can manipulate the time and date of their activities, making it difficult to accurately determine when a crime occurred. Third, the evidence aspect of cybercrime is problematic because the object sought is not only the device, but also the traces, identities, and data used to prepare, commit, and produce the crime; in the open nature of the internet system, parties with technical capabilities can disguise or falsify identities, even hijack or clone systems illegally, so that data can be manipulated—for example, changing fake data to appear authentic. In this context, questions also arise regarding who can be brought forward as witnesses for legal events that occur on the internet, for example, whether employees of service providers or platform managers (web designers, programmers, data entry, and

[22] I. Koto, "Cyber Crime According to the ITE Law," *International Journal Reglement & Society (IJRS)* 2, no. 2 (2021): 103–10, https://doi.org/https://doi.org/10.55357/ijrs.v2i2.124.

other employees) can testify about violations such as defamation, insults, fraud, pornography, and other unlawful acts (Sitompul).

Fourth, the nature of cybercrime, which is often committed by a lone perpetrator in a closed space,[23] makes it difficult for investigators to obtain witnesses who directly witnessed the incident,[24] so that evidence often relies on the victim's testimony. In certain cases, such as in the banking sector, there is also a tendency for institutions to withhold information about attacks because it is considered that it could damage reputations and reduce public trust. Fifth, the jurisdictional aspect is becoming increasingly complex because state jurisdiction in the conventional sense is based on geographical boundaries, while multimedia communication is cross-border, multi-jurisdictional, and borderless, so that the application of law enforcement authority has the potential to create a tug-of-war between countries that both feel disadvantaged. In addition to these normative and technical challenges, handling cybercrime is also limited by the capacity of law enforcement officers, both in terms of human resources and the availability of infrastructure; even a special unit to handle cybercrime within the Indonesian National Police was only formed in a more structured manner at the Criminal Investigation Agency level through the Cyber Crime Directorate in February 2017, while previously handling cybercrime was still within the special economic crime unit.

Proof and evidence are fundamental aspects that determine the direction and outcome of the criminal justice process,[25] because it is through proof that material truth is assessed and criminal responsibility can be established.[26] As new forms of crime emerge that utilize digital media and increasingly diverse modus operandi,[27] the criminal procedural law system is required to make adjustments to remain able to accommodate these developments. In the Indonesian context, one important normative response is the extension of evidence from the conventional evidence regime as regulated in Article 184 paragraph (1) of the Criminal Procedure Code, through the recognition of electronic evidence. This strengthening is emphasized in Article 44 of the ITE Law, which recognizes electronic information and electronic documents as part of the evidence that can be used in the criminal justice process.

However, the application of electronic evidence as valid evidence in the Indonesian criminal justice system still faces a number of vulnerabilities. These obstacles include the difficulty in precisely establishing the locus delicti and tempus delicti, issues of authenticity and integrity of electronic data, limited availability of direct witnesses, jurisdictional issues in cross-border crimes, and varying capacities of law enforcement officials—both in terms of technical competence and infrastructure—in effectively handling and proving cyber cases.

---

[23] Nick Nykodym, Robert Taylor, and Julia Vilela, "Criminal Profiling and Insider Cyber Crime," *Computer Law & Security Review* 21, no. 5 (2005): 408–14, https://doi.org/10.1016/j.diin.2005.11.004.

[24] Alice Hutchings and Ben Collier, "Inside out : Characterising Cybercrimes Committed inside and Outside the Workplace," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).*, 2019, 481–90, https://doi.org/10.1109/EuroSPW.2019.00060.

[25] Walter P. Signorelli, *Criminal Law, Procedure, and Evidence*, 2nd Edition (New York: Routledge, 2023), https://doi.org/https://doi.org/10.4324/9781003415091.

[26] Artem Rudin Kostenko, Roman V., "Notion and Meaning of Evidence Verification in Criminal Procedure," *Journal of Advanced Research in Law and Economics* 9, no. 3 (2018): 1011–17, https://doi.org/https://www.ceeol.com/search/article-detail?id=735315.

[27] B. E. Turvey, "Modus Operandi, Motive, and Technology," in *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (Netherlands: Elsevier, 2011), 285–304.

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 10, No. 2-December 2025

E. Conclusions

This research shows that the dynamics of cybercrime in Indonesia are evolving faster than the legal system's ability to anticipate them. The increasingly complex digital landscape demands a prevention mechanism that relies not only on regulatory instruments but also on a technological foundation capable of proactively and in real-time identifying potential threats. These findings emphasize that cybercrime prevention can no longer be considered an additional effort but should be a core structure within the national cyber law framework.

On the other hand, the analysis shows that the current legal framework is still oriented toward post-incident handling. This paradigm leaves the state always one step behind cybercriminals, especially when attacks utilize cutting-edge technology. This weakness is not only a normative issue but also a consequence of the lack of technical standards to guide relevant institutions. Therefore, continuity between regulations and technical operational mechanisms is a strategic priority if prevention goals are to be achieved effectively.

The reconstruction of the cybercrime prevention model proposed by this research positions information technology as a central instrument, not merely a supplement. The presence of machine learning, threat intelligence, data-based monitoring systems, and early detection algorithms provides significant opportunities to create a more responsive and adaptive legal system. This technological integration not only enhances the country's ability to anticipate attacks but also accelerates the mitigation process before wider losses occur.

Furthermore, strengthening cybercrime prevention and response in Indonesia needs to be directed towards an integrated model that combines technical capabilities and legal certainty. The national legal framework already provides a crucial foundation, particularly through the recognition of electronic evidence and data protection obligations. However, its effectiveness remains limited due to the lack of uniform operational standards for early warning, the absence of a structured incident reporting mechanism based on severity, and the suboptimal management of CTI and the integration of incident data across sectors. Therefore, regulatory harmonization and strengthening measurable governance are key to ensuring that cybercrime management is not a one-size-fits-all approach but develops into a proactive, responsive, and evidence-based national cyber resilience system.

Furthermore, this research demonstrates the need for harmonization between national law and international standards as part of efforts to build a robust prevention system. Cyber threats are cross-border and cannot be addressed with a partial or fragmented approach. Alignment between domestic regulations, international cooperation mechanisms, and global data governance offers significant benefits in strengthening Indonesia's position in the cybersecurity realm.

Overall, this research contributes by offering a new direction in developing a more comprehensive cybercrime prevention model. It underscores that the success of developing a national cyber law system depends on its readiness to holistically integrate technological and regulatory tools. Therefore, this research is expected to serve as a foundation for developing more preventative and innovative national policies capable of addressing future cybersecurity challenges.

REFERENCES

Aminah, Sitti, Herie Saksono. "Digital Transformation of the Government: A Case Study in Indonesia." In *Jurnal Komunikasi: Malaysian Journal of Communication*, 37:272–88, 2021. https://doi.org/https://doi.org/10.1007/978-3-031-36001-5_37.

Asyari, Haekal Al. "Between Freedom And Protection: A Critical Review Of Indonesia'S Cyberspace Law." *Prophetic Law Review* 5, no. 1 (2023): 79–103. https://doi.org/https://doi.org/10.20885/PLR.vol5.iss1.art5.

Butt, S. "Indonesia's Criminal Justice System on Trial: The Jessica Wongso Case." *New Criminal Law Review* 24, no. 1 (2021): 3–58. https://doi.org/https://doi.org/10.1525/nclr.2021.24.1.3.

Hamzani, A. I., Widyastuti, T. V., Khasanah, N., & Rusli, M. H. M. "Legal Research Method: Theoretical and Implementative Review." *International Journal of Membrane Science and Technology* 10, no. 2 (2023): 3610–19.

Hunter, D. "Cyberspace as Place and the Tragedy of the Digital Anticommons." In *Law and Society Approaches to Cyberspace*, 59–139, 2017. https://doi.org/https://www.taylorfrancis.com/chapters/edit/10.4324/9781351154161-3/cyberspace-place-tragedy-digital-anticommons-dan-hunter.

Hutchings, Alice, and Ben Collier. "Inside out : Characterising Cybercrimes Committed inside and Outside the Workplace." In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).*, 481–90, 2019. https://doi.org/10.1109/EuroSPW.2019.00060.

Kharlie, Ahmad Tholabi, Muhammad Ishar Helmi. "The Role of the Law on Electronic Information and Transactions in Overcoming Challenges of Democracy in Indonesia." *International Journal of Advanced Science and Technology* 28, no. 20 (2019): 1178–84. https://doi.org/https://fathudin85.wordpress.com/wp-content/uploads/2020/02/3505-article-text-5555-1-10-20200120.pdf.

Kirillova, E. A., Bogdan, V. V., Golovatskaya, M. V., Melnichenko, T. A., & Ognev, V. N. "Legal Significance of Electronic Messages and Documents." *Journal of Advanced Research in Law and Economics* 9, no. 3 (2018): 997–1003. https://doi.org/https://www.ceeol.com/search/article-detail?id=735202.

Kostenko, Roman V., Artem Rudin. "Notion and Meaning of Evidence Verification in Criminal Procedure." *Journal of Advanced Research in Law and Economics* 9, no. 3 (2018): 1011–17. https://doi.org/https://www.ceeol.com/search/article-detail?id=735315.

Koto, I. "Cyber Crime According to the ITE Law." *International Journal Reglement & Society (IJRS)* 2, no. 2 (2021): 103–10. https://doi.org/https://doi.org/10.55357/ijrs.v2i2.124.

Kraemer-Mbula, Erika, Puay Tang, Howard Rush. "The Cybercrime Ecosystem: Online Innovation in the Shadows?" *Technological Forecasting and Social Change* 80, no. 3 (2013): 541–55. https://doi.org/https://doi.org/10.1016/j.techfore.2012.07.002.

Lagazio, M., Sherif, N., & Cushman, M. "A Multi-Level Approach to Understanding the Impact of Cyber Crime on the Financial Sector." *Computers & Security* 45 (2014): 58–74. https://doi.org/https://doi.org/10.1016/j.cose.2014.05.006.

Negara, T. A. S. "Normative Legal Research in Indonesia: Its Originis and Approaches." *Audito Comparative Law Journal (ACLJ)* 4, no. 1 (2023): 1–9. https://doi.org/https://doi.org/10.22219/aclj.v4i1.24855.

Nykodym, Nick, Robert Taylor, and Julia Vilela. "Criminal Profiling and Insider Cyber Crime." *Computer Law & Security Review* 21, no. 5 (2005): 408–14.

https://doi.org/10.1016/j.diin.2005.11.004.

Paterson, Thomas. "Indonesian Cyberspace Expansion: A Double-Edged Sword." *Journal of Cyber Policy* 4, no. 2 (2019): 216–34. https://doi.org/https://doi.org/10.1080/23738871.2019.1627476.

Ramesh, S. K. A., & Kiran, S. "AI-Enhanced Cyber Threat Detection." *International Journal of Computer Trends and Technology (IJCTT)* 72, no. 6 (2024): 64–71. https://doi.org/https://doi.org/10.14445/22312803/IJCTT-V72I6P109.

Satoto, E., & Santiago, F. "Reconstruction of Indonesia's Cyber Law System for Adaptive and Integrated Digital Crime Prevention in the Era of Technological Disruption." *Greenation International Journal of Law and Social Sciences* 3, no. 2 (2025): 309–17. https://doi.org/https://doi.org/10.38035/gijlss.v3i2.425.

Signorelli, Walter P. *Criminal Law, Procedure, and Evidence*. 2nd Editio. New York: Routledge, 2023. https://doi.org/https://doi.org/10.4324/9781003415091.

Sivakumar, Janaki and Salman, Nawras Rafid and Salman, Farah Rafid and Salimova, Husniya Rustamovna and Ghimire, Enjina. "AI-Driven Cyber Threat Detection : Enhancing Security through Intelligent Engineering Systems." *Journal of Information Systems Engineering and Management* 10, no. 19 (2025): 790–98. https://doi.org/https://doi.org/10.52783/jisem.v10i19s.3116.

Sulistyani, W. "The Admissibility of Scientific Expert Evidence under Indonesian Criminal Justice System." *Sriwijaya Law Review* 3, no. 2 (20919): 152–61. https://doi.org/https://doi.org/10.28946/slrev.Vol3.Iss2.215.pp152-161.

Sunaryo, S. "The Meaning of'against Justice'in Judicial Decisions of Criminal Cases in Indonesia." *International Journal of Public Law and Policy* 10, no. 4 (2024): 359–82. https://doi.org/https://doi.org/10.1504/IJPLAP.2024.141710.

Taherdoost, Hamed. "Insights into Cybercrime Detection and Response: A Review of Time Factor." *Information* 15, no. 5 (2024): 273. https://doi.org/https://doi.org/10.3390/info15050273.

Thomas, D., & Loader, B. D. "Introduction: Cybercrime: Law Enforcement, Security and Surveillance in the Information Age." In *Cybercrime*, 1–14. Routledge, 2013.

Turvey, B. E. "Modus Operandi, Motive, and Technology." In *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 285–304. Netherlands: Elsevier, 2011.

Viano, E. C. "Cybercrime: Definition, Typology, and Criminalization." In *Cybercrime, Organized Crime, and Societal Responses: International Approaches*, 3–22, 2016. https://doi.org/https://doi.org/10.1007/978-3-319-44501-4_1.