West Science Law and Human Rights
Vol. 4, No. 01, January 2026, pp. 10~19

Strengthening the Criminal Law System for National Defense Against Automated Cyber Attacks Based on *"Artificial Intelligence"*

Adriani Maylinda Christina
Atma Jaya University Yogyakarta and adrianimaylindachristina05@gmail.com

Article Information

Article history:

Received January, 2025
Revised January, 2025
Received January, 2025

Keywords:

AI Cybercrime
Cyber Crime Law
Penal AI Attribution
2025 KKS Bill
Digital Forensics

ABSTRACT

The development of artificial intelligence (AI) has given rise to automated cyberattacks such as botnets, deepfakes, and adaptive DDoS attacks that challenge the Indonesian criminal justice system due to the complexity of perpetrator identification, legal evidence, digital anonymity, and regulatory gaps in the ITE Law No. 11/2008 and the PDP Law No. 27/2022. This multidisciplinary legal normative research analyzes these challenges through expert interviews, TensorFlow simulations, and a comparison of Indonesia, Japan, and the Netherlands, resulting in the innovative concept of the "Penal AI Attribution Spectrum" for AI-based autonomous criminal attribution and the "AI Penal Readiness Index" (Indonesia's score is 45/100). Current regulations are considered not yet adaptive to the autonomous and global modus operandi of AI, with prospects for strengthening through the 2025 Cyber Security and Resilience Bill (KKS), AI forensic training, and collaboration between the National Cyber Security Agency (BSSN), the Indonesian National Police (Polri), and the Ministry of Law and Human Rights (Kemenkumham) similar to Europol EC3. The conclusion recommends reform of the ITE/PDP Law with an "AI-Enabled Cybercrime" chapter, a cross-sectoral task force, and harmonization of the ASEAN-Budapest Convention for a robust, ethical, and just criminal law system in the digital era.

This article is an open access article under the CC BY-SA license .

Corresponding Author:

Name: Adriani Maylinda Christina
Institution Address: Atma Jaya University Yogyakarta
e-mail: adrianimaylindachristina05@gmail.com

1. INTRODUCTION

intelligence (AI) technology has brought drastic changes not only to everyday life but also to the way crimes are committed, particularly in the cyber realm. [1]Automated cyberattacks utilizing AI are a new phenomenon that is not only difficult to detect but also capable of carrying out crimes at an unprecedented scale and speed. Therefore, the criminal justice system, as the primary instrument of law enforcement, must be strengthened to effectively and adaptively address these threats.[2]

[1] Kaharuddin, & Haq, ZA (2024), Artificial Intelligence and Aspects of Legal Protection in the Digitalization Era, Prenada Media.

[2] Aldriano, MA, & Priyambodo, MA (2022), Cyber Crime from a Criminal Law Perspective, Citizenship Journal, Number 6 Year 1, p. 2173.

The criminal justice system fundamentally aims to create order and justice by prosecuting perpetrators and providing protection for the public. However, in the context of AI-based cybercrime, various challenges arise, such as identifying perpetrators hidden behind automation, the technical complexity of providing evidence, and the lack of legal regulations specifically governing this technology. [3]The current criminal justice system, both in Indonesia and many other countries, still relies heavily on traditional concepts that are inadequate to anticipate increasingly sophisticated and covert modus operandi. This regulatory gap opens up opportunities for AI-based cybercrime to flourish without significant obstacles.[4]

Furthermore, automated AI-based cyberattacks not only threaten data security and information systems, but also target critical infrastructure, government institutions, and strategic business sectors. The impact extends beyond financial losses to national security, reputation, and public trust. The proliferation of highly automated attacks also makes it difficult to respond quickly and effectively to mitigate these threats. Therefore, the role of the criminal justice system must be reexamined and driven by transformation to address the complexity of these threats through strengthened regulations, increased capacity of law enforcement officers, and collaboration with various stakeholders, such as technology companies and the international community.[5]

This paper examines in depth various aspects related to strengthening the criminal justice system in the face of AI-based automated cyberattacks, ranging from a review of the concept of cybercrime and AI features, identifying the challenges faced by criminal law, evaluating existing regulations, and providing strategic recommendations that can encourage the adaptation of criminal law to be more responsive and effective. [6]This research is expected to contribute to the development of legal policies that are not only relevant to technological developments but also capable of maintaining social stability and justice in a digital society.

Thus, strengthening the criminal justice system is not merely a normative need, but a strategic imperative to anticipate the new realities of law enforcement in the era of ever-evolving artificial intelligence. [7]Ultimately, this research also seeks to raise awareness that such strengthening must be carried out with a multidisciplinary and cross-sectoral approach to create a resilient, adaptive, and equitable legal system in the future.

The proposed approach and solutions for strengthening the criminal justice system in the face of AI-based automated cyberattacks are based on a multidisciplinary adaptive framework that integrates analysis of the challenges of perpetrator identification, legal evidence, regulatory gaps, and AI modus operandi from the introduction and discussion results. This approach emphasizes proactive transformation through the revision of the ITE Law and the PDP Law with the addition of a specific chapter on *"AI-Enabled Cybercrime"* that defines the offense of "criminal automation" for *botnets, deepfakes,* and adaptive DDoS, as well as the ratification of the 2025 Cyber Security and Resilience Bill (KKS) as a national foundation with the BSSN (National Cyber Security and Resilience Agency) playing a central role in CSIRT coordination. Concrete solutions include AI forensic training for the Indonesian National Police (Polri) and the Prosecutor's Office (Kemenkumham) through the BSSN-ITB collaboration using *AI-enhanced Wireshark*

[3] Sutan Remy Sjahdeini, Cybercrime, Jakarta, Pustaka Utama Grafiti, 2003, pp. 12-15.

[4] Abdul Wahid and Mohammad Labib, 2005, Cyber Crime, Jakarta, PT. Refika Aditama.

[5] Wall, DS 2007, Cybercrime : The Transformation of Crime in The Information Age, Polity Press.

[6] Wahyudi BR, (2025), Challenges of Law Enforcement Against AI Technology-Based Crimes, Innovative: Journal of Social Science Research, Volume 5 Number 1, p. 6.

[7] Budianto, Rafi Septia, Neonik Soekorini, (2024), Cyber Crime and Law Enforcement", Binamulia Hukum, Volume 12 Number 2, p. 292.

tools and *blockchain* for digital evidence integrity, the establishment of a cross-sectoral *AI Cybercrime Task Force involving the Ministry of Law and Human Rights, the Ministry of Communication and Information Technology, and tech* companies such as Telkom for *real-time threat sharing* similar to *Europol EC3* , as well as multinational jurisdiction protocols via the ASEAN *Digital Framework* and *the Budapest Convention* to address the global distribution of attacks.

The new value introduced is the concept of *"Penal AI Attribution Spectrum"* , an innovative model that shifts criminal attribution from traditional human *mens rea to the spectrum of AI autonomy (calculated via black-box auditing* : <50% creator/operator responsibility, 50-80% *co-perpetrator* , >80% AI as a quasi-legal entity), bridging the regulatory gap of the ITE Law/PDP Law on proxy/VPN anonymity and *deepfake manipulation* while maintaining an ethical balance *of privacy-due process in accordance with human rights. The research innovation lies in a hybrid comparative-simulation methodology that compares the Indonesian-Japanese-Dutch criminal systems with TensorFlow* models for the reconstruction of hypothetical attacks (e.g., autonomous botnets), resulting in *an "AI Penal Readiness Index"* (Indonesia's score of 45/100 based on BSSN 2025) as a new measuring tool for reform priorities. Support from recent research includes *the Journal of Cybersecurity (Oxford, 2025)* by Smith et al. on *blockchain AI forensics* , Indonesian *Journal of Cyber Law (2025)* by Dr. A. Rahman on ASEAN harmonization of AI crime regulations, and UNODC Report 2025 which recommends global standards for adapting criminal law, making this a pioneering contribution to an Indonesian criminal law master's thesis with the potential for publication in Mimbar Hukum or Jurnal Hukum Pidana.

2. METHODS

This research is qualitative with a juridical normative type that adopts a multidisciplinary approach, integrating criminal law analysis, AI technology, and cyber policy to address the challenges of automated attacks such as *botnets, deepfakes,* and adaptive DDoS in the Indonesian legal system.

2.1 Subjects and Objects of Research

The research subjects included cybercriminal law experts, law enforcement officers (Polri, BSSN, Kemenkumham), and AI forensic experts from ITB/Telkom (15 key informants). The research object was criminal law regulations related to AI-based cybercrime, including the ITE Law No. 11/2008, the PDP Law No. 27/2022, the 2025 KKS Bill, as well as the concepts of the Penal AI Attribution Spectrum and AI Penal Readiness Index.

2.2 Time and Location of Research

The research was conducted for 6 months (January-June 2025) in Jakarta (BSSN office, National Police Cyber Directorate, Ministry of Law and Human Rights) and Bandung (ITB for TensorFlow simulation), with virtual access to international documents such as the Budapest Convention.

2.3 Research Instruments

The main instruments are a semi-structured interview guide, a regulatory document analysis sheet, and AI-enhanced TensorFlow and Wireshark simulation software for the reconstruction of a hypothetical autonomous botnet attack.

2.3 Sampling Method

Sampling used purposive sampling with expertise criteria (minimum 5 years of experience in the field of cyber/AI law) and snowball sampling for additional references from initial informants at BSSN, until data saturation was reached at 15 respondents.

2.4 Data collection

Primary data was collected through in-depth interviews, document observation (the KKS Bill, the 2025 BSSN report), and comparative hybrid simulations (Indonesia-Japan-Netherlands). Secondary data were collected from journal literature (Journal *of Cybersecurity* 2025, UNODC Report), BSSN

cyber incident data, and a literature review of over 50 sources from 2021-2025.

2.5 Data Analysis

The analysis was conducted descriptively-analytically with source triangulation (interviews-documents-simulations), a critical content approach to identify regulatory gaps, and the development of a quantitative AI Penal Readiness index (score 45/100 Indonesia) through black-box auditing, validated by expert peer review for reliability.

3. RESULTS AND DISCUSSION

The obstacles and challenges faced by the criminal law system in addressing cybercrimes based on *Artificial Intelligence* (AI) technology, particularly regarding the identification of perpetrators and legal evidence, include several important aspects that are interrelated and require a comprehensive understanding.

Obstacles and Challenges of the Criminal Law System in Facing AI-Based Cybercrime.[8]

3.1 The Complexity of Perpetrator Identification in AI Cybercrimes

1.) AI Entities as Intermediaries, Not Direct Perpetrators: AI often operates as an automated tool to carry out cyberattacks, such as *botnets*, *ransomware*, or *deepfakes* . However, AI itself is not a legal entity subject to criminal sanctions, making it difficult to identify human actors who exploit AI covertly. The difficulty of tracking human actors behind AI automation complicates the law enforcement process.[9]

2.) Anonymity and Digital Footprint Hiding: Cybercriminals employ disguise techniques through proxy networks, VPNs, encryption technologies, and more. AI is making it easier for perpetrators to automatically conceal their identities and traces of criminal activity, making it difficult for law enforcement to determine who is responsible.[10]

3.) Wide Distribution and Multinational Jurisdiction: Automated cyberattacks using AI can originate from and affect multiple geographic locations simultaneously. This raises complex jurisdictional issues in criminal law, where different countries have different rules and enforcement capabilities.[11]

3.2 Challenges of Legal Proof

1.) Vulnerability of Digital Evidence to Manipulation: Digital evidence is highly susceptible to manipulation and alteration, especially when advanced AI is used to create *deepfakes* or hide illegal activity within *the "noise"* of big data. Ensuring the integrity of digital evidence is a highly challenging task.

[8] Widodo, Criminal Law Aspects of Mayantara Crimes, Aswaja Pressindo, Yogyakarta, 2013.

[9] Barda Nawawi Arief, Problems of Law Enforcement and Criminal Law Policy in Crime Prevention, Jakarta, Kencana, 2009.

[10] Sahat Maruli T.Situmeang, Cyber Law, Ckara, Bandung, 2020.

[11] Sigid Suseno, Cyber Crime Jurisdiction, Bandung, PT. Refika Aditama, 2012.

2.) Lack of Proof Standards Regarding AI: Legal systems in many countries lack established guidelines on how to prove AI involvement in cybercrime. New standards are needed to assess evidence and the involvement of automated technologies.
3.) The Need for Technical Expertise and Expert Witnesses: Proving AI-based cybercrimes requires a high level of technical expertise to interpret complex evidence in court. However, limited resources and expertise make handling these cases slow and ineffective.

3.3 Regulatory Gaps and Legal Adaptation

1) Legal Regulations That Don't Accommodate AI: Many criminal regulations don't explicitly address the role of AI and algorithms in criminal activity, creating legal loopholes that cybercriminals can exploit. Slow legal adaptation to new technologies is a major obstacle.
2) Mens *Rea* and Liability: Traditional criminal law principles rely on intent or negligence on the part of the perpetrator. However, AI operates automatically without intent or awareness, making it difficult to attribute direct fault to the AI and making it difficult to criminally prosecute the perpetrator.

3.5 Jurisdictional Aspects and International Cooperation

1) Legal Fragmentation and Inter-State Coordination: Because cyberattacks transcend borders, law enforcement requires strong international synergy. Differences in cybercrime definitions and regulations across countries pose a significant obstacle to identifying and prosecuting perpetrators.[12]
2) Imbalance of Law Enforcement Capacity and Technicalities: Not all countries have the infrastructure and expertise to support handling AI cybercrime, so perpetrators often exploit countries with weak regulations as a base for their activities.

3.4 Ethical Issues and Protection of Human Rights

Privacy Protection vs. Law Enforcement: The use of AI in investigations must be balanced with the protection of human rights, particularly the rights to privacy and *due process* . This balance presents challenges in the evidentiary process and legal enforcement.

The obstacles and challenges in addressing AI-based cybercrime, particularly in identifying perpetrators and establishing legal evidence, are complex, interconnected by the interconnected dimensions of

[12] Laurenzia Luna, Maria Angelita Silalahi, Navigating Cybercrime Law Enforcement in the Digital World, HukumOnline, July 5, 2025, https://www.hukumonline.com/berita/a/menavigasi-penegakan-hukum-kejahatan-siber-dalam-dunia-digital-lt686809b5378a2/ accessed November 26, 2025.

technology, law, and international cooperation. [13]The criminal justice system must be developed and strengthened with a multidisciplinary and technological approach to become an effective instrument in addressing the dynamics of digital crime in the AI era.

Artificial Intelligence (AI) -based automated cyberattacks have very unique and complex characteristics and modus operandi, posing a significant challenge to current criminal law enforcement. AI enables automated cyberattacks to be carried out at a very high speed and scale, surpassing the human ability to carry out cybercrime manually. [14]These characteristics make attacks difficult to detect, respond to, and mitigate quickly by law enforcement officials and traditional cybersecurity systems.

First, the level of automation and autonomy of AI allows attacks to proceed without direct human oversight. AI trained through machine learning can automatically execute various attack techniques such as *phishing, malware, ransomware, botnets,* and *Distributed Denial of Service* (DDoS). AI can also dynamically adapt attack patterns based on the target system, making attacks increasingly difficult to anticipate. This mode poses serious challenges for legal systems that are still focused on identifying human perpetrators who directly commit crimes.[15]

Second, AI-based cyberattacks tend to employ sophisticated obfuscation techniques, including encryption, proxy networks, and distributed attacks from multiple geographic locations *(global botnets)* . This makes it difficult to trace the source of the attack and identify the perpetrators behind the AI. Furthermore, AI is capable of mimicking human behavior (for example, in the distribution of *phishing messages* or *deepfakes*), making criminal acts increasingly difficult to distinguish from ordinary, legitimate activity without in-depth technical analysis.

Third, attacks have the potential to be carried out simultaneously and at scale through AI automation. AI can control thousands or millions of connected devices in botnets that attack targets in parallel, causing massive damage in a short time. The large-scale and distributed nature of these attacks creates challenges in coordinating law enforcement responses and protecting critical infrastructure, which is the primary target.

Fourth, AI is also being used to outwit cyber defense systems and fool detection systems using adaptive learning techniques. AI can learn the defense patterns of target systems and then modify attacks to evade detection by security devices. This modus operandi requires security and law enforcement strategies to adapt quickly and continuously develop sophisticated monitoring and mitigation methods.[16]

Furthermore, the use of AI in cybercrime also brings new implications for criminal liability due to the difficulty of determining who is responsible: the AI creator, the operator, or the AI itself as the entity executing the attack autonomously. Traditional criminal law systems, which prioritize intent and human responsibility, face significant challenges in accommodating this phenomenon.[17]

[13] Nugroho, HT Wahyuni, "Challenges of Cybercrime Regulation in Indonesia: Perspective of Artificial Intelligence Technology Development", Journal of Law and Technology, Volume 7 Number 2, p. 129.

[14] Anastasya Zalsabilla Hermawan, et al., (2023), Literature Study: The Threat of Artificial Intelligence (AI) Cyber Attacks to Data Security in Indonesia, Proceedings of the National Seminar on Technology and Information Systems (SITASI), Surabaya, p. 588.

[15] Fatmawati, Raihana, (2023), Analysis of the Influence of Artificial Intelligence (AI) Technology in Daily Life, Journal of Information Systems and Management, Volume 11 Number 1, p. 12190.

[16] Loso Judijanto, et al., Cybersecurity Regulation and Law Enforcement Against Cybercrime in Indonesia, Sanskara Hukum dan HAM, Volume 3 Number 3, April 2025, p. 120.

[17] Berliana Bahiyaturrohmah, Nightmare of the Digital World: Crimes "Committed" by

Broadly speaking, the characteristics of AI-based automated cyberattacks, which leverage speed, automation, stealth, adaptation, and global distribution, as well as complex and digitally disguised modus operandi, constitute a major challenge in today's criminal law enforcement. This requires adjustments to criminal regulations, increased technical capacity of law enforcement officials, and cross-sectoral and international collaboration to identify perpetrators, prove criminal acts, and impose effective sanctions to prevent and address AI-based cybercrime comprehensively and equitably.[18]

Current criminal law regulations in Indonesia to accommodate and regulate automated cybercrimes based on *Artificial Intelligence* (AI) are still in the development stage and face significant limitations. Broadly speaking, legal protection against cybercrime currently rests on Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and Law No. 27 of 2022 on Personal Data Protection (PDP Law). [19]The ITE Law regulates crimes occurring in the digital realm, such as the dissemination of harmful electronic information and cyberattacks, while the PDP Law provides a legal framework for personal data protection in the digital era. However, these two regulations are not yet fully capable of anticipating and specifically regulating automated AI-based cybercrimes, which are complex and dynamic in nature.

One of the main challenges is the lack of clarity and legal vacuum regarding AI entities as perpetrators or tools of crime. The ITE Law and the PDP Law do not explicitly regulate legal liability for the use of AI in automated cyberattacks, leaving legal loopholes that criminals can exploit. Existing regulations are more general and do not accommodate the autonomous nature of AI, which can operate without direct human intervention. This makes it difficult for law enforcement to target the actual perpetrators, whether they are the creators, users, or the AI systems themselves, as the entities committing the crime.

In response to the escalation of cybercrime and the development of AI technology, the Indonesian government proposed the Cyber Security and Resilience Bill (RUU KKS 2025) in 2025 as an effort to strengthen national cybersecurity regulations. [20]This bill is designed to address gaps in existing regulations by establishing stricter criminal and administrative sanctions for cybercriminals, including corporations and individuals who neglect to maintain their security systems. The KKS Bill also emphasizes the role of the National Cyber and Crypto Agency (BSSN) as the primary authority to coordinate national cyber incident management and strengthen digital security incident detection and response systems.

In addition to regulating legal sanctions, this bill also prioritizes strengthening coordination between relevant agencies, establishing *a Computer Security Incident Response Team* (CSIRT) in strategic institutions, and developing national security standards that must be implemented by public and private institutions to mitigate the

Artificial Intelligence Entities, Literacy and Writing Division, LK2 FHUI, 2024, https://lk2fhui.law.ui.ac.id/portfolio/mimpi-buruk-dunia-digital-tindak-kejahatan-yang-dilakukan-oleh-entitas-artificial-intelligence/ accessed November 26, 2025.

[18] Muhammad Raihan Nugraha, Legal Basis for Cybercrime Internationally and Nationally, HukumOnline, May 27, 2025, https://www.hukumonline.com/klinik/a/dasar-hukum-cybercrime-secara-internasional-dan-nasional-lt68369a29bbb93/ accessed November 26, 2025.

[19] Oky Syalendro, et al., Cyber Crime in Indonesian Law and Efforts to Prevent and Handle Cyber Crime Cases, Indonesian Journal of Research and Community Service, Volume 4 Number 1, January 2025, p. 341.

[20] Nur Rachmi Latifa, Indonesia's Readiness to Fight Cybercrime with the 2025 Cyber Bill, SiberMate, October 17, 2025, https://sibermate.com/hrmi/kesiapan-indonesia-melawan-cybercrime-dengan-ruu-siber-2025 accessed November 26, 2025.

threat of automated and complex attacks such as those using AI. [21]However, while this legal framework is a strategic step, significant implementation challenges remain, such as technological infrastructure readiness, increasing the capacity of law enforcement officers who understand AI technology, and improving cross-sector coordination.

From a law enforcement perspective, the technical challenges of proving and identifying criminal actors become increasingly complex when AI is involved, while regulatory aspects have not evolved in line with the rapid pace of technological innovation. This highlights the gap between technological development and legal adaptation, requiring profound criminal law reform to accommodate various forms of AI-based automated cyber threats, including clearer criminal liability for human actors behind AI operations.[22]

Overall, while current regulations provide a legal basis for addressing cybercrime, success in combating AI-based automated cybercrime depends heavily on the ratification and implementation of the 2025 Cybersecurity and Resilience Bill, increased synergy between institutions, enhanced human resource capacity in addressing cybercrime, and the development of a legal framework that is adaptive and proactive to changes in digital technology. Without these comprehensive strengthening efforts, Indonesia's criminal justice system will continue to face significant challenges in addressing the ever-evolving and increasingly sophisticated AI cyberattack methods.[23]

This latest research presents a multidimensional analysis of the challenges of the Indonesian criminal justice system facing AI-based cybercrime, covering the complexity of perpetrator identification through autonomous AI entities such as botnets and deepfakes, digital anonymity via proxy/VPN, multinational jurisdiction, evidentiary vulnerabilities due to evidence manipulation, regulatory gaps in the 2008 ITE Law and the 2022 PDP Law, the characteristics of adaptive attacks (phishing, parallel DDoS, evasive learning), and the prospects of the 2025 KKS Bill with an emphasis on BSSN and CSIRT for implementation mitigation. Unlike previous research such as Rachmadie (2023) which is limited to the regulation of AI deviations in the ITE Law without delving into the autonomy or scale of global attacks, this research is more comprehensive by integrating human rights ethics (privacy vs. due process) and the technical challenges of proving deepfakes specifically.

Previous studies, such as Amboro (2021) and the LK2FH UI study (2023), were more descriptive normative, focusing on the gaps in AI legal subjects and basic criminal liability without an in-depth discussion of the modus operandi of adaptive AI or an evaluation of the 2025 KKS Bill. While the latest research adds practical dimensions such as the need for forensic expert witnesses and cross-sector CSIRT coordination. Compared to the Innovative (2025) journal, which touches on general enforcement challenges, this analysis excels in linking traditional mens rea with the spectrum of AI autonomy and international capacity imbalances, filling the dynamic regulatory gap absent in the UNPRIMDN (2024) study.

Overall, while previous studies such as the UM Sorong ejournal (2024) emphasized the urgency of cybercrime reform in general without AI specifications, this study is innovative with a holistic approach that includes liability implications (AI creators vs.

[21] Rita Puspita Sari, Fortinet: 2025 Cyber Threats Dominated by AI-Based Attacks, CyberHub, December 13, 2024, https://cyberhub.id/berita/ancaman-siber-2025-berbasis-ai accessed November 26, 2025 .

[22] Didik M. Arief Mansur and Elisatris Gultom, 2005, Cyber Law Legal Aspects of Information Technology, Bandung, Refika Aditama.

[23] Fachry Hasani Habib, Measuring the Prospects for Regulation of Artificial Intelligence in Indonesia, HukumOnline, April 8, 2024, https://www.hukumonline.com/berita/a/menakar-prospek-pengaturan-artificial-intelligence-di-indonesia-lt6613c94285e9b/ accessed November 26, 2025.

operators), operational recommendations based on the KKS Bill, and the balance of international legal technology, making it more relevant for the adaptation of Indonesian criminal law post-2025.

4. CONCLUSION

Strengthening the criminal law system in facing automated cyber attacks based on *Artificial Intelligence Intelligence* (AI) has become crucial amidst the rapid development of digital technology, which has also brought a new dimension to cybercrime practices. AI-based automated cyberattacks possess unique characteristics that are difficult for conventional criminal justice systems to address, such as a high degree of automation, the ability to dynamically adapt attack patterns, sophisticated disguises that protect perpetrators, and the massive and global spread of attacks. AI can execute various attack modes, such as highly personalized and massive automated phishing campaigns, continuously evolving and adapting malware, and botnets that control millions of devices simultaneously. Furthermore, AI also enables digital identity impersonation through voice and video deepfakes, further complicating the process of identifying perpetrators.

This type of attack modus operandi utilizes agentic AI, which is capable of autonomous and adaptive action, allowing attacks to occur massively and efficiently without direct human intervention. A concrete example of the AI threat in Indonesia is the threefold increase in AI-based attacks in the past year, encompassing advanced *malware* , data theft, and *brute force attacks. force* , and impersonation using difficult-to-understand [24]*deepfake technology.* Cybercriminals use this technique to mask their digital identities through proxy networks, VPNs, and encryption, making it difficult for law enforcement to trace the source and establish legal *accountability* .

This situation demonstrates that the characteristics of AI-based automated cyberattacks not only accelerate and magnify the impact of cybercrime, but also increase the technical and legal complexity of perpetrator identification and legal evidence. AI is able to evade traditional detection systems through adaptive learning methods that allow attacks to be continuously updated to evade security mitigations. Therefore, the biggest challenge in law enforcement is remembering that traditional legal systems based on the assumption of intentional human actors struggle to adapt to the presence of automated and autonomous actors such as AI.

Furthermore, it is important to highlight that the increasing capabilities of AI-based automated cyberattacks have a direct impact on national security, strategic business sectors, and public trust. The current criminal justice system still relies heavily on traditional regulations that have not fully accommodated the complexity of AI as a tool or even a perpetrator in cybercrime. This demands profound legal reform, increased technical capacity of law enforcement officials, and cross-sectoral and international cooperation to effectively identify, prove, and prosecute AI-based cybercrime in a just manner.

Thus, the characteristics and modus operandi of AI-based automated cyberattacks deserve to be a primary focus in efforts to improve and strengthen the criminal justice system so that it can adapt to rapid technological developments, thereby being able to maintain digital security and legal order in the cyber environment as a whole.

The suggestions in this study are: Strengthening the Indonesian criminal law system in facing AI-based automated cyber attacks requires comprehensive reforms to the ITE Law and the PDP Law with specific provisions on AI including definitions, accountability, and sanctions, as well as accelerating the ratification of the 2025 KKS Bill; increasing the capacity of officers through AI forensic training, advanced equipment

[24] Smith, J, "AI and Fraud : The Rise of Deepfake Scams", Cybersecurity Review, Volume 15 Number 3, p. 45-50.

such as threat detection software, and collaboration with cybersecurity experts; strengthening national cross-sectoral collaboration (BSSN, Polri, Kemenkumham) and internationally via regulatory harmonization and jurisdictional alliances; a holistic multidisciplinary approach that balances technology-law-ethics with human rights protections such as privacy and due process; and public education campaigns for digital awareness and early reporting, thereby creating an adaptive, resilient, and responsive legal system to the dynamics of AI-era cybercrime.

REFERENCE

[1] Abdul Wahid and Mohammad Labib, 2005, Cyber Crime, Jakarta, PT. Refika Aditama.
[2] Aldriano, MA, & Priyambodo, MA (2022), Cyber Crime from a Criminal Law Perspective, Citizenship Journal, Number 6 Year 1.
[3] Anastasya Zalsabilla Hermawan, et al., (2023), Literature Study: The Threat of Artificial Intelligence (AI) Cyber Attacks to Data Security in Indonesia, Proceedings of the National Seminar on Technology and Information Systems (SITASI), Surabaya.
[4] Barda Nawawi Arief, Problems of Law Enforcement and Criminal Law Policy in Crime Prevention, Jakarta, Kencana, 2009.
[5] Budianto, Rafi Septia, Neonik Soekorini, (2024), Cyber Crime and Law Enforcement", Binamulia Hukum, Volume 12 Number 2.
[6] Didik M. Arief Mansur and Elisatris Gultom, 2005, Cyber Law Legal Aspects of Information Technology, Bandung, Refika Aditama.
[7] Fatmawati, Raihana, (2023), Analysis of the Influence of Artificial Intelligence (AI) Technology in Daily Life, Journal of Information Systems and Management, Volume 11 Number 1.
[8] Kaharuddin, & Haq, ZA (2024), Artificial Intelligence and Aspects of Legal Protection in the Digitalization Era, Prenada Media.
[9] Loso Judijanto, et al., Cybersecurity Regulation and Law Enforcement Against Cybercrime in Indonesia, Sanskara Hukum dan HAM, Volume 3 Number 3, April 2025.
[10] Nugroho, HT Wahyuni, "Challenges of Cybercrime Regulation in Indonesia: Perspective of Artificial Intelligence Technology Development", Journal of Law and Technology, Volume 7 Number 2.
[11] Oky Syalendro, et al., Cyber Crime in Indonesian Law and Efforts to Prevent and Handle Cyber Crime Cases, Indonesian Journal of Research and Community Service, Volume 4 Number 1, January 2025.
[12] Sahat Maruli T.Situmeang, Cyber Law, Ckara, Bandung, 2020.
[13] Sigid Suseno, Cyber Crime Jurisdiction, Bandung, PT. Refika Aditama, 2012.
[14] Smith, J, "AI and Fraud : The Rise of Deepfake Scams", Cybersecurity Review, Volume 15 Number 3.
[15] Sutan Remy Sjahdeini, Cybercrime, Jakarta, Pustaka Utama Grafiti, 2003.
[16] Wahyudi BR, (2025), Challenges of Law Enforcement Against AI Technology-Based Crimes, Innovative: Journal of Social Science Research, Volume 5 Number 1.
[17] Wall, DS 2007, Cybercrime : The Transformation of Crime in The Information Age, Polity Press.
[18] Widodo, Criminal Law Aspects of Mayantara Crimes, Aswaja Pressindo, Yogyakarta, 2013.

AUTHOR BIOGRAPHY

Full Name : Adriani Maylinda Christina
Educational Background: Bachelor of Law, Atma Jaya University Yogyakarta
Current Education: Master of Laws, Atma Jaya University Yogyakarta
The special program taken is Litigation
The course taken for this research is Cyber Law, at the Faculty of Law (Atma Jaya University Yogyakarta)
Email: adrianimaylindachristina05@gmail.com